

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail, in an envelope addressed to: Commissioner for Patents, Washington, DC 20231, on the date shown below.

Dated: February 11, 2003

Signature:

*Andrew T. Zidel*  
(Andrew T. Zidel)

#9  
1-36-04  
JM  
Docket No.: SONYTA 3.3-139  
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:  
Asano et al.

Application No.: 09/937,120

Group Art Unit: 2131

Filed: December 17, 2001

Examiner: Not Yet Assigned

For: DATA PROCESSING APPARATUS AND  
DATA PROCESSING METHOD

Commissioner for Patents  
Washington, DC 20231

**REQUEST TO AMEND DRAWINGS**

Dear Sir:

Further to applicant's amendment dated February 11, 2003, permission is requested to amend the drawings of the above-identified application as indicated in red on the copy of the drawings attached hereto. By the requested changes, applicants seek to correct mislabeled elements, to add headings, and to correct typographical errors. Accordingly, applicants submit that none of these amendments will add new matter to the disclosure of the present application and, therefore, that these amendments should be enterable.

If the Examiner has any questions with respect to the proposed changes, he is invited to telephone the undersigned at (908) 654-5000. Additionally, if there are any fees due and owing, the Examiner is authorized to charge our Deposit Account No 12-1095 therefor.

Dated: February 11, 2003

Respectfully submitted,

By

*Andrew T. Zidel*

Andrew T. Zidel

Patent Agent

Registration No.: 45,256

LERNER, DAVID, LITTENBERG,  
KRUMHOLZ & MENTLIK, LLP

600 South Avenue West  
Westfield, New Jersey 07090  
(908) 654-5000  
Attorneys for Applicant

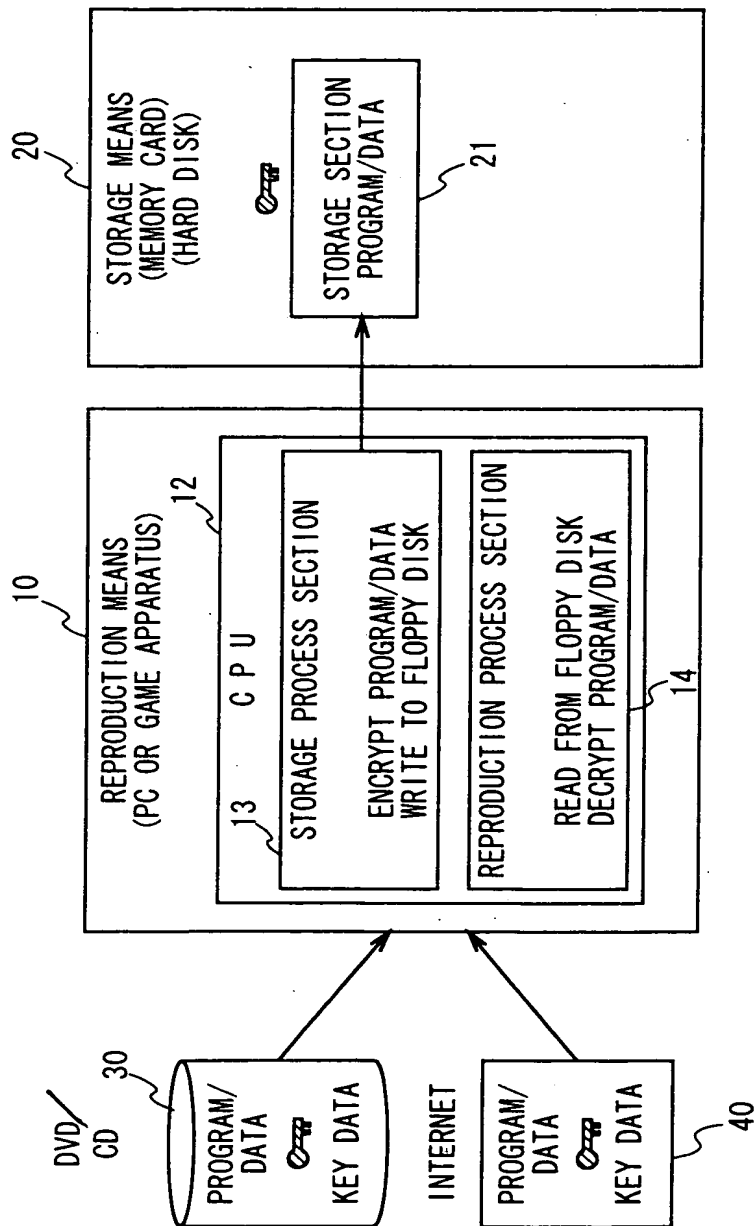


FIG. 1

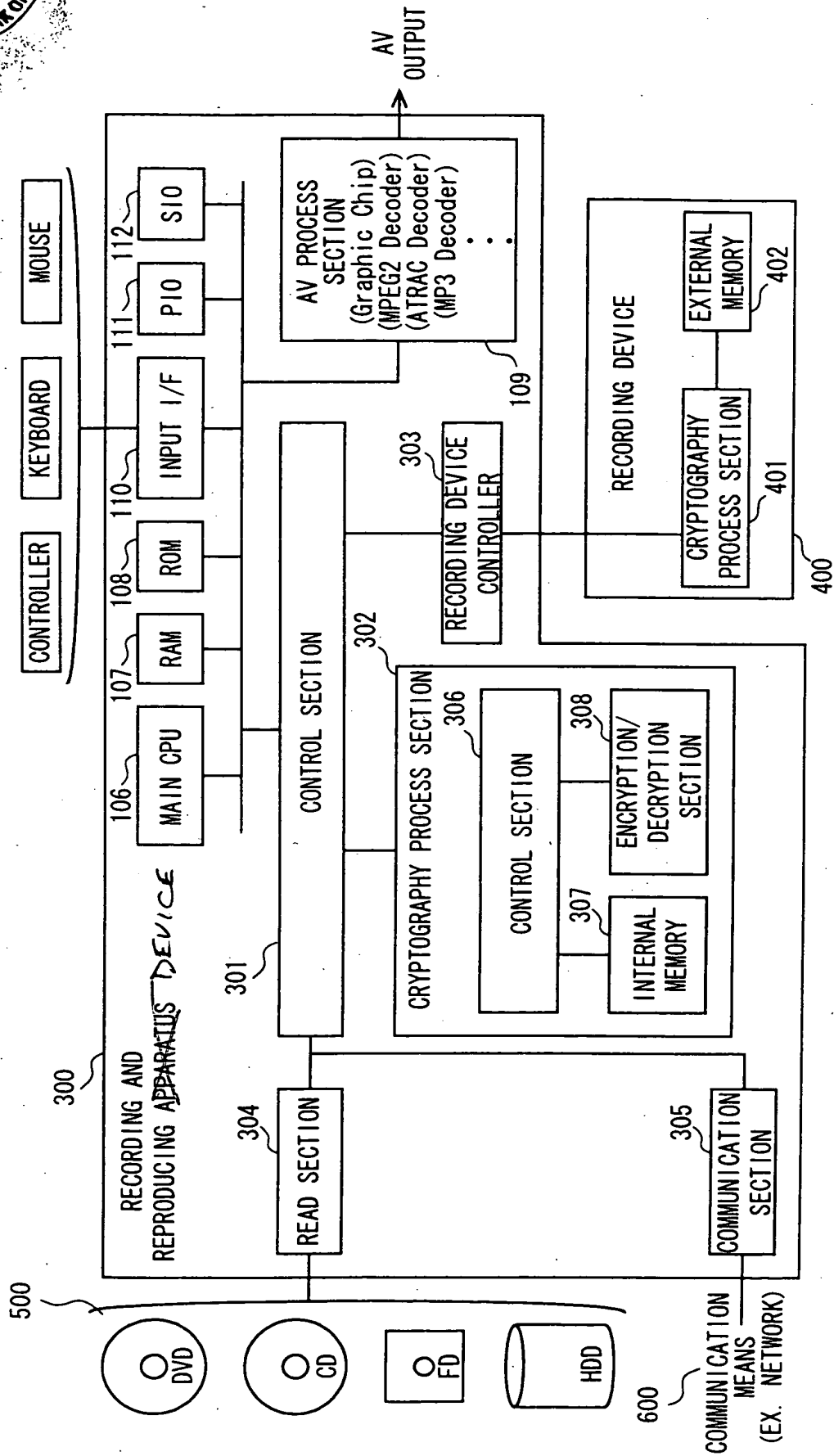


FIG. 2

COMMUNICATION

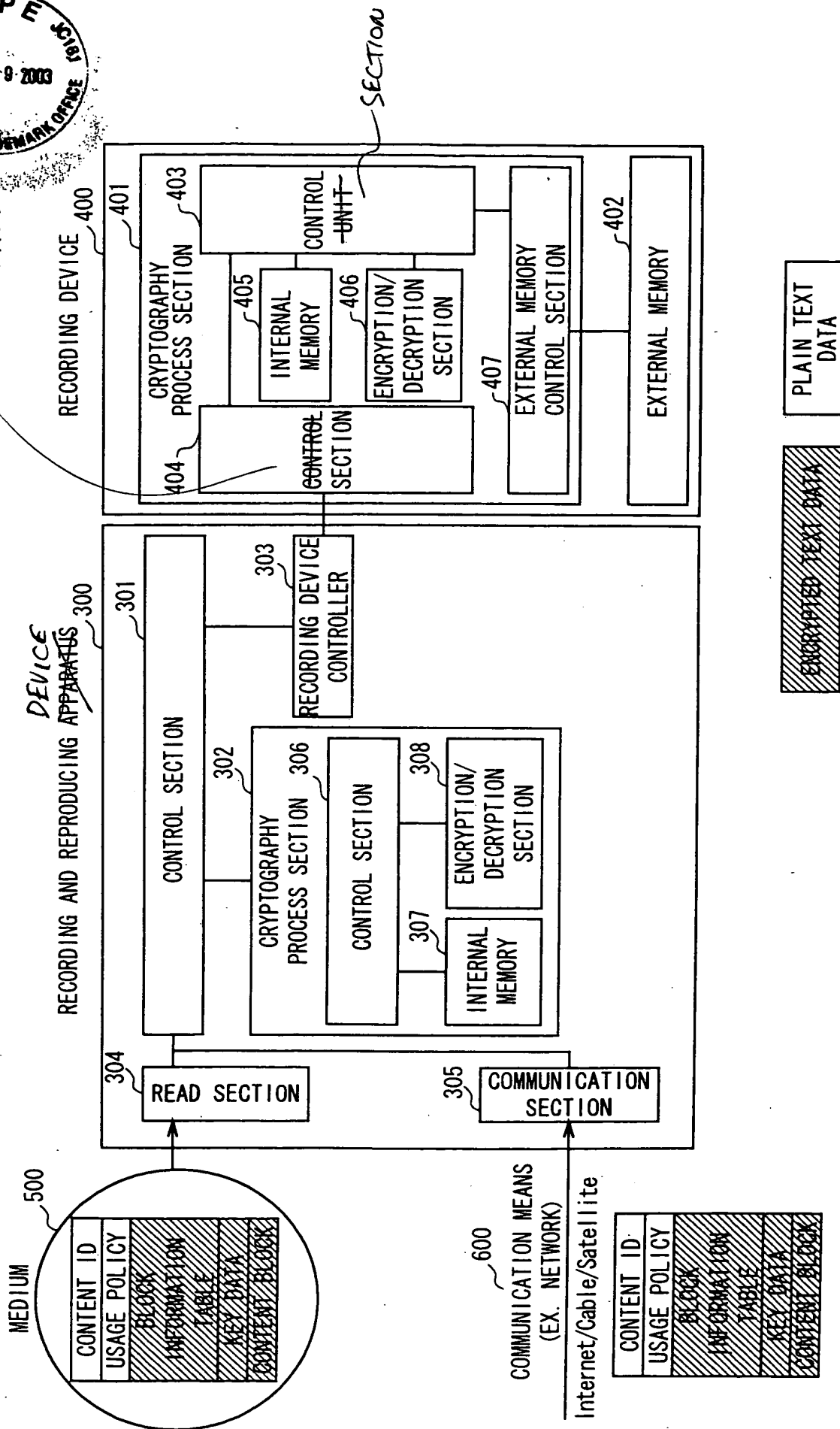
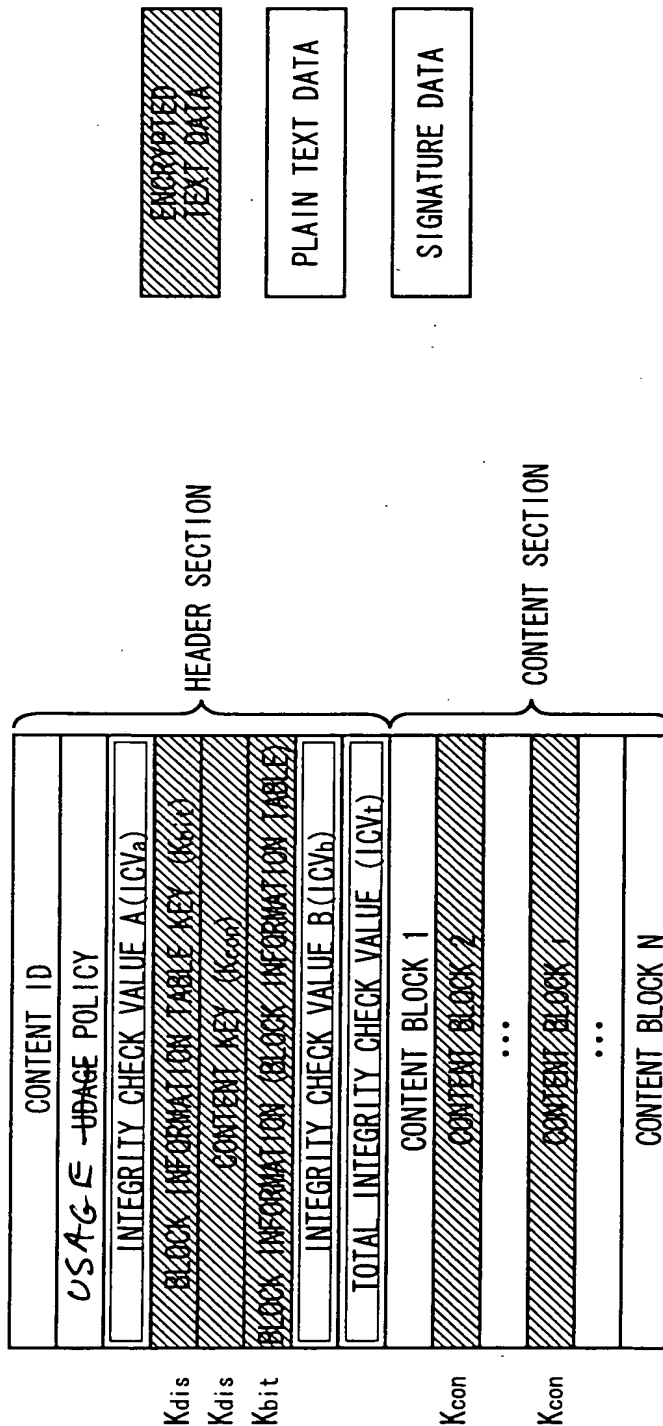
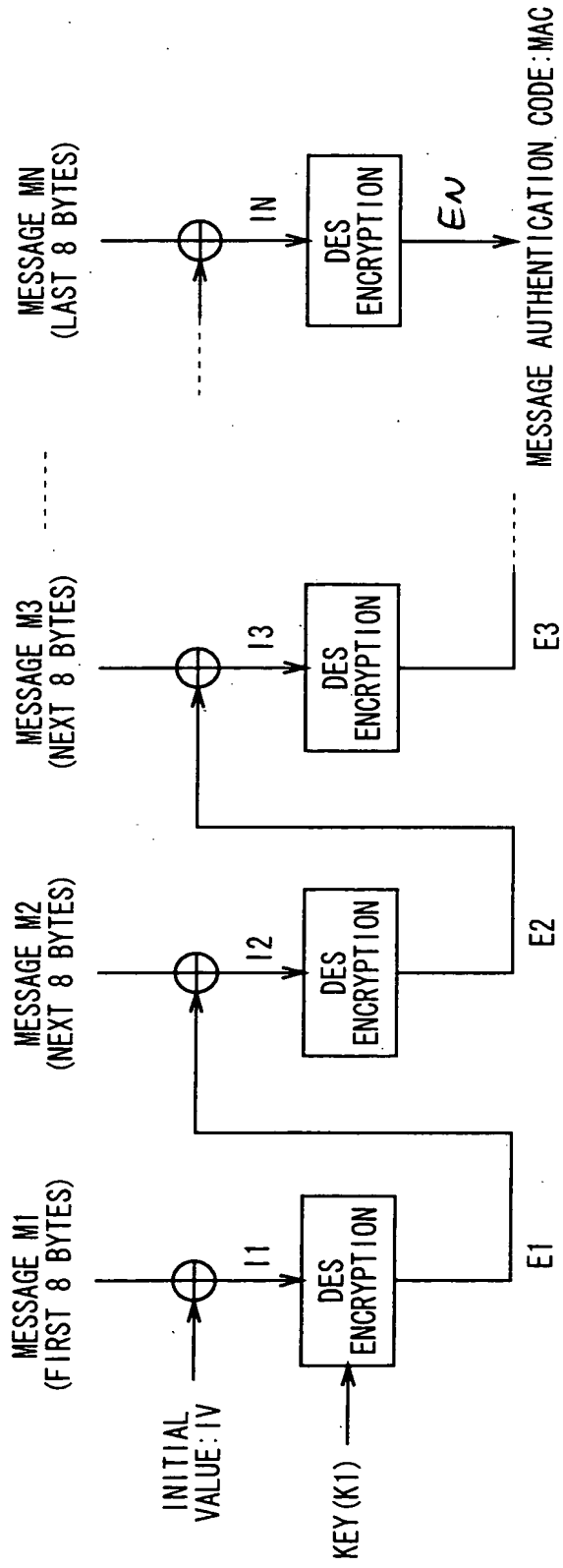


FIG. 3



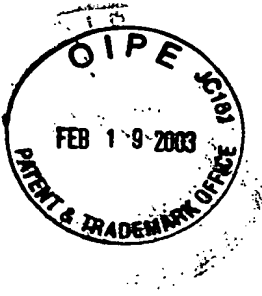
DATA FORMAT ON MEDIUM AND COMMUNICATION PATH

FIG. 4

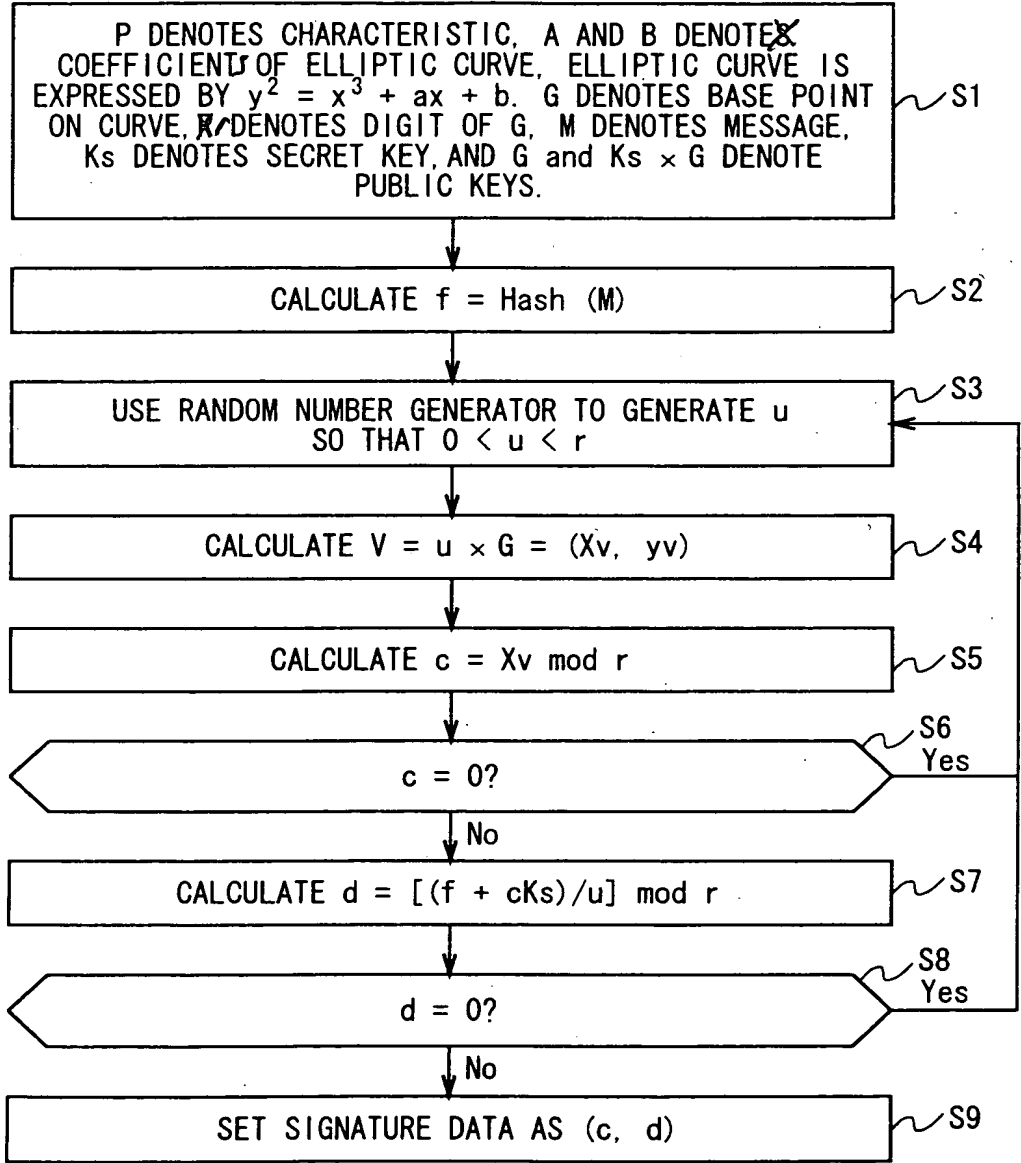


⊕: EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 7



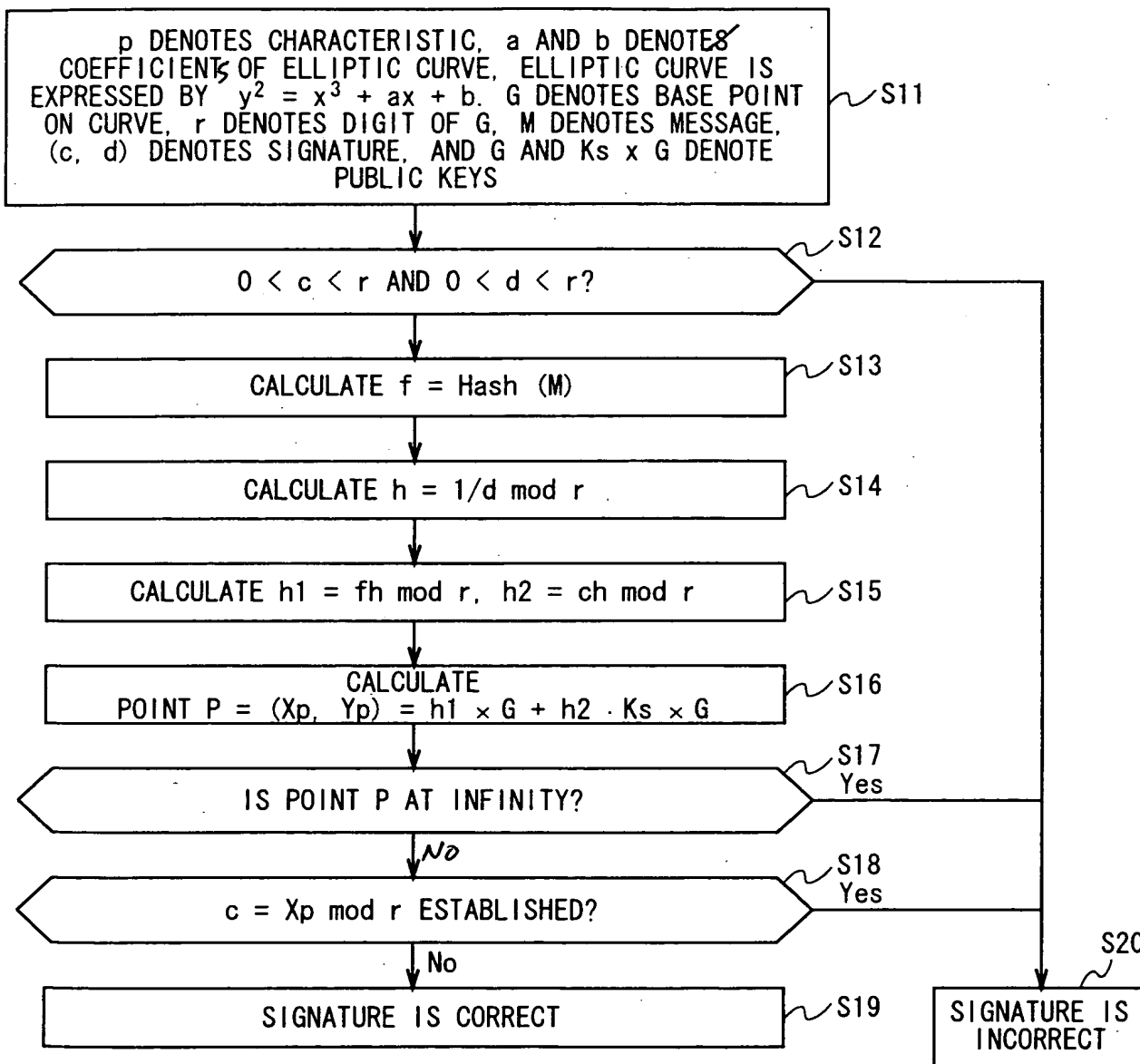
SIGNATURE GENERATION



GENERATION OF SIGNATURE (IEEE P1363/D3)

FIG. 11

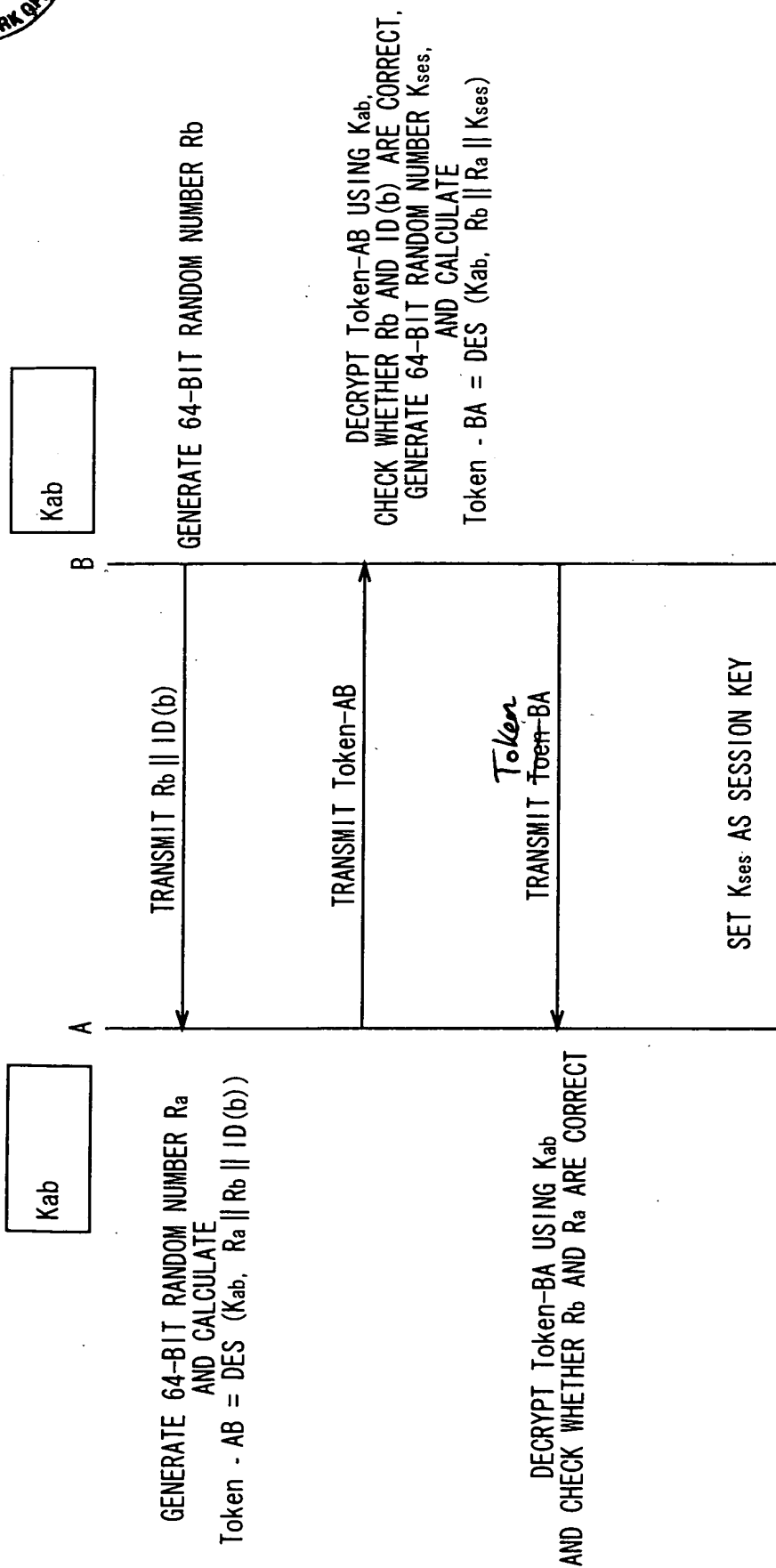
# SIGNATURE VERIFICATION



SIGNATURE VERIFICATION(IEEE P1363/D3)

FIG. 12

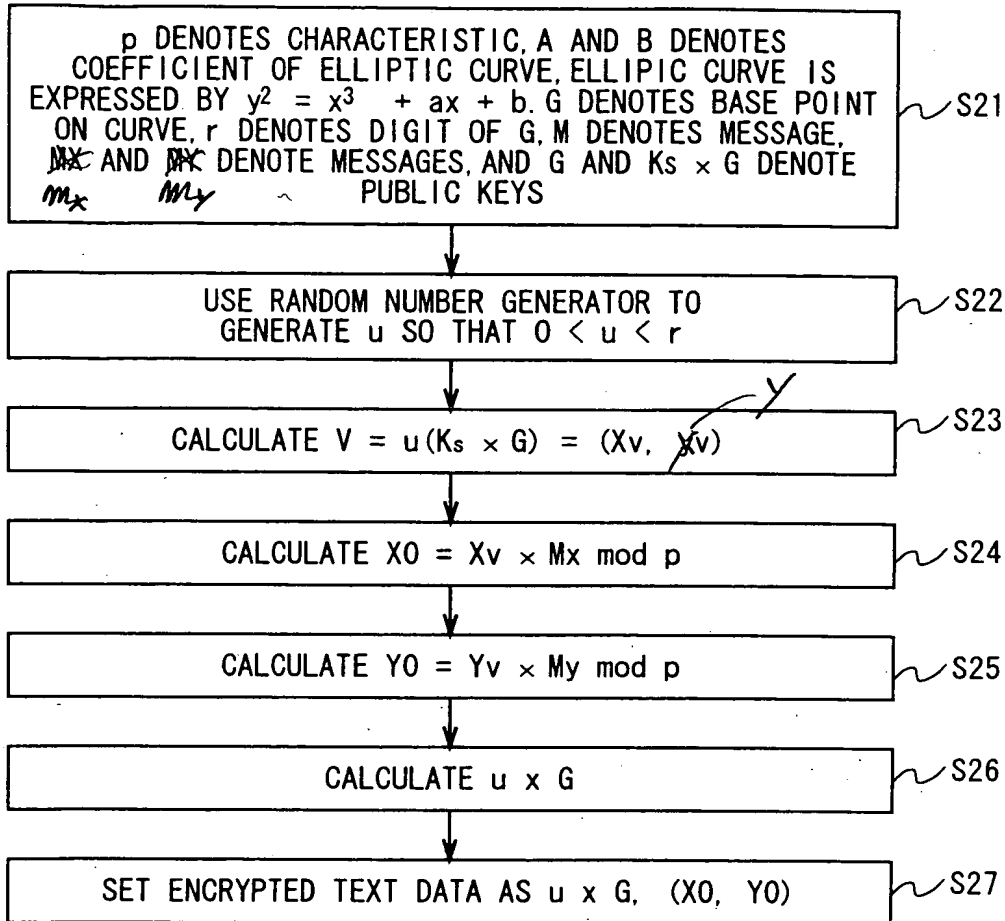






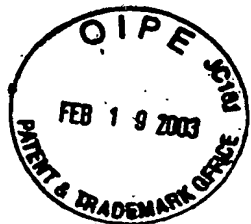


## ENCIPHERMENT

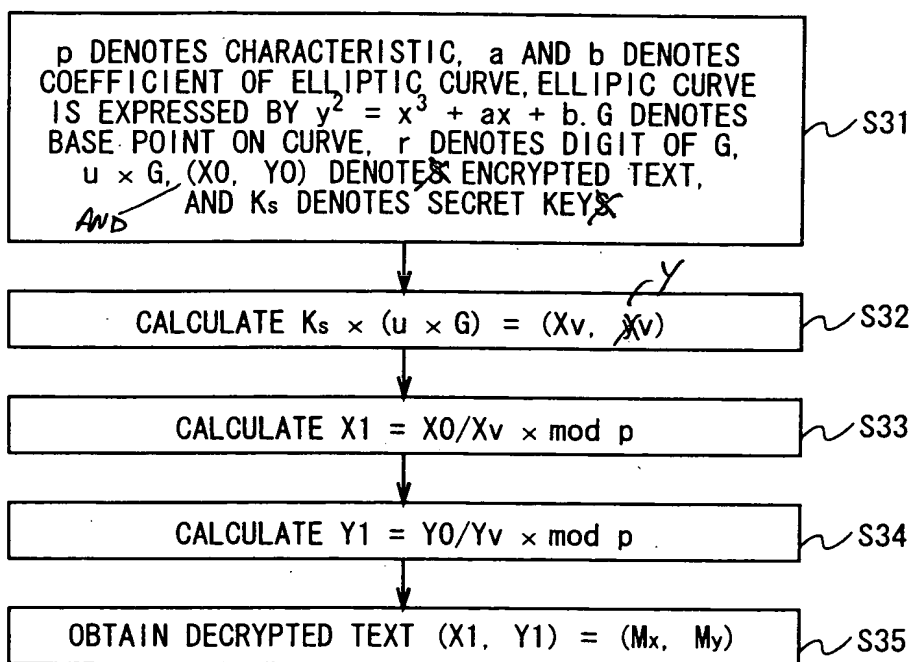


## ENCIPHERMENT USING ELLIPTIC CURVE CRYPTOGRAPHY (MENEZES-VANSTONE)

FIG. 16

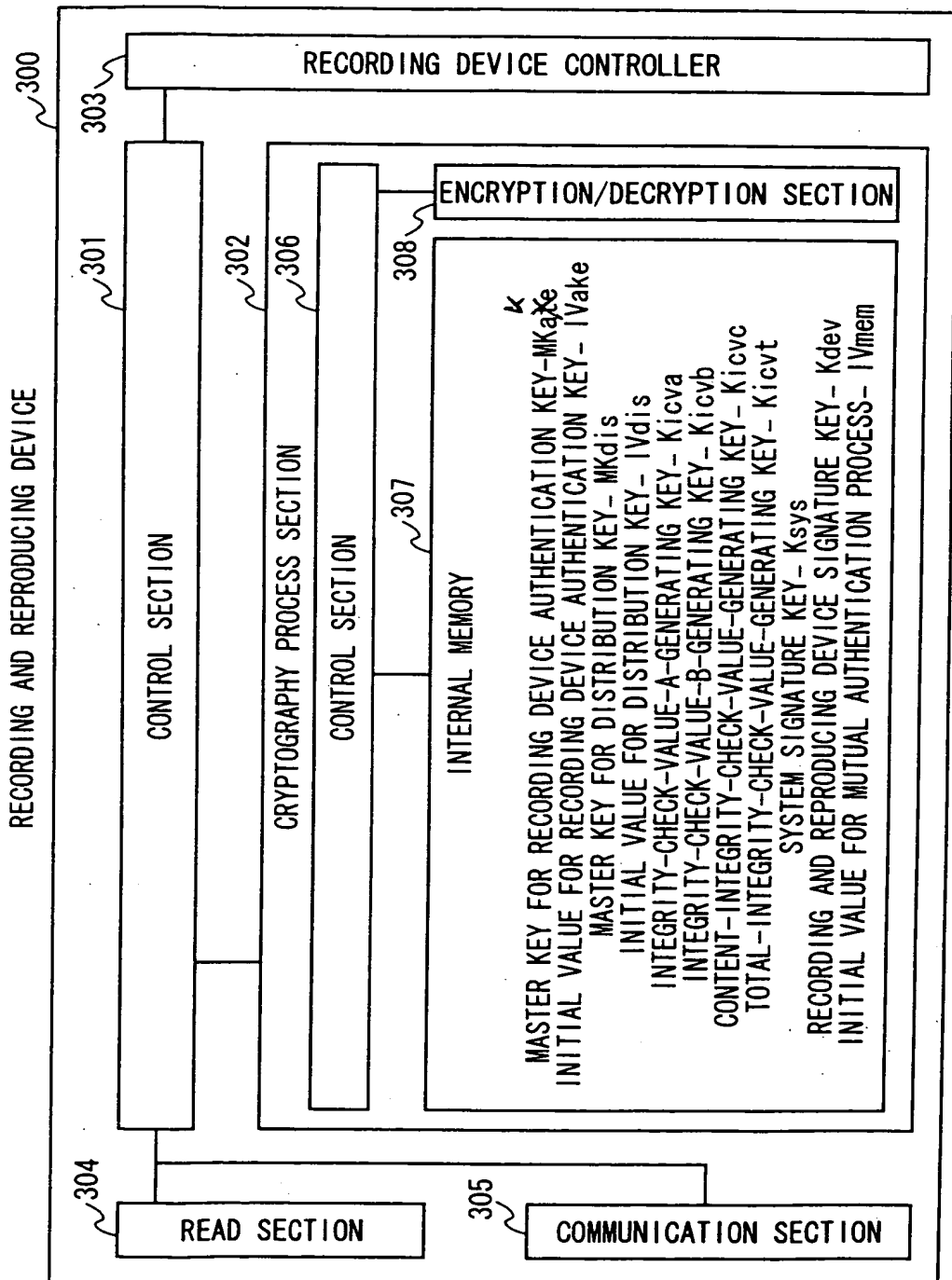


### DECRYPTION



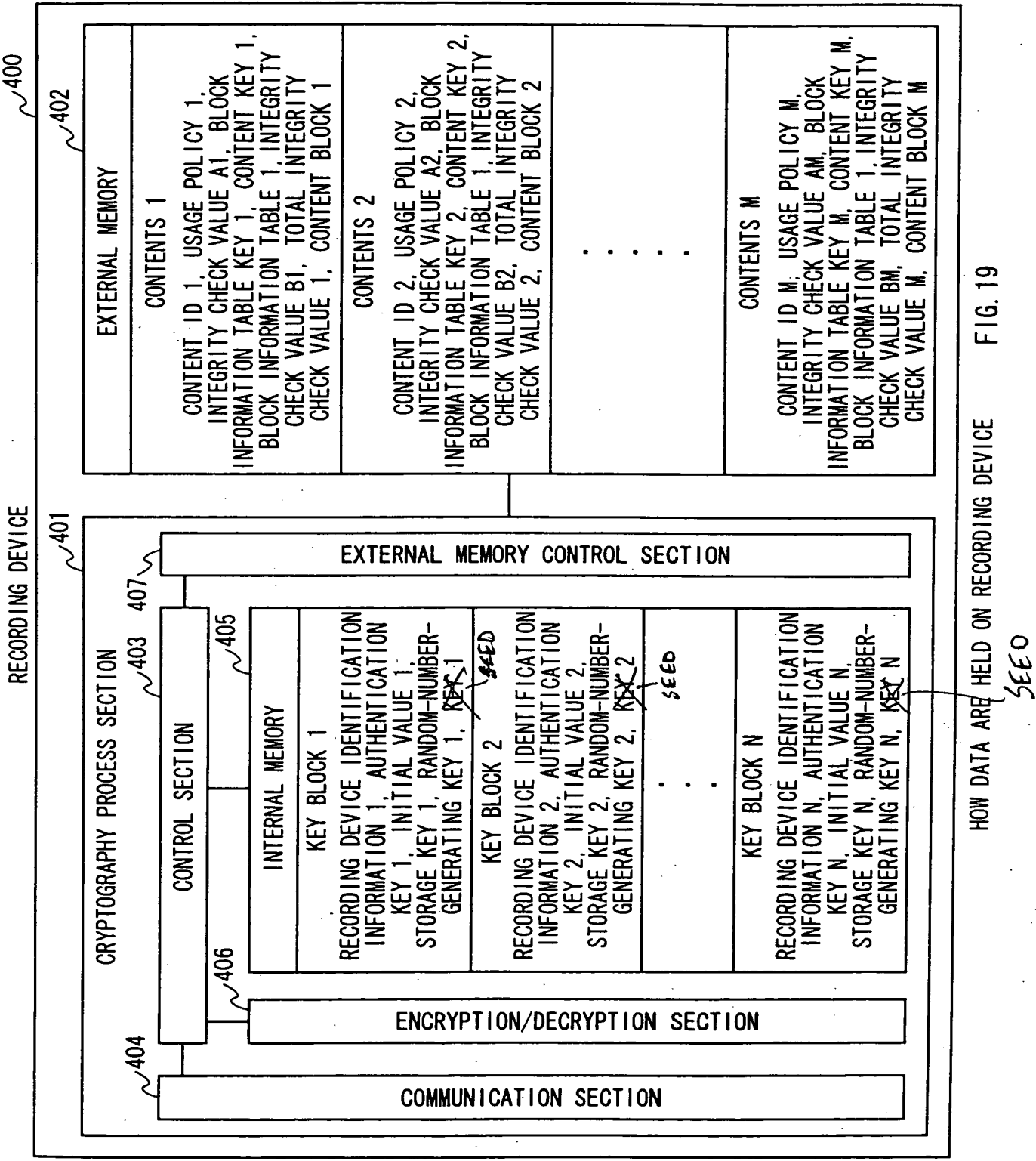
DECRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY (MENEZES-VANSTONE)

FIG. 17



HOW DATA ARE HELD ON RECORDING AND REPRODUCING DEVICE

FIG. 18



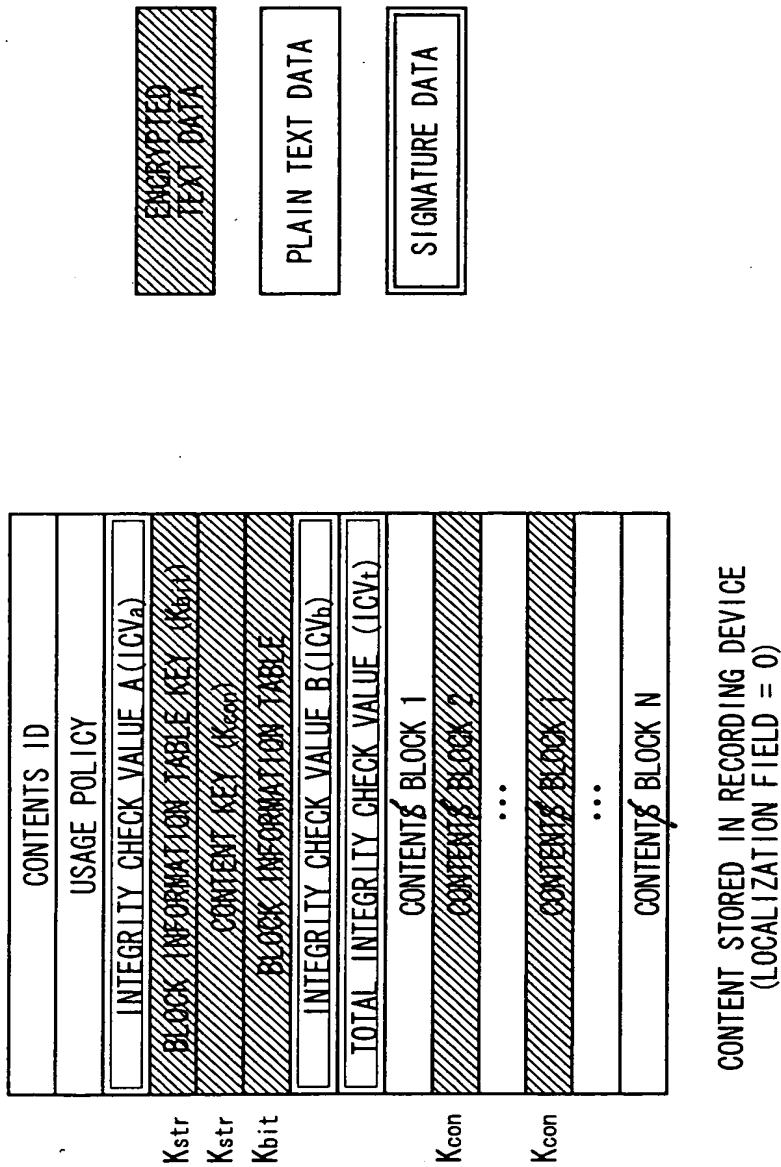


FIG. 26

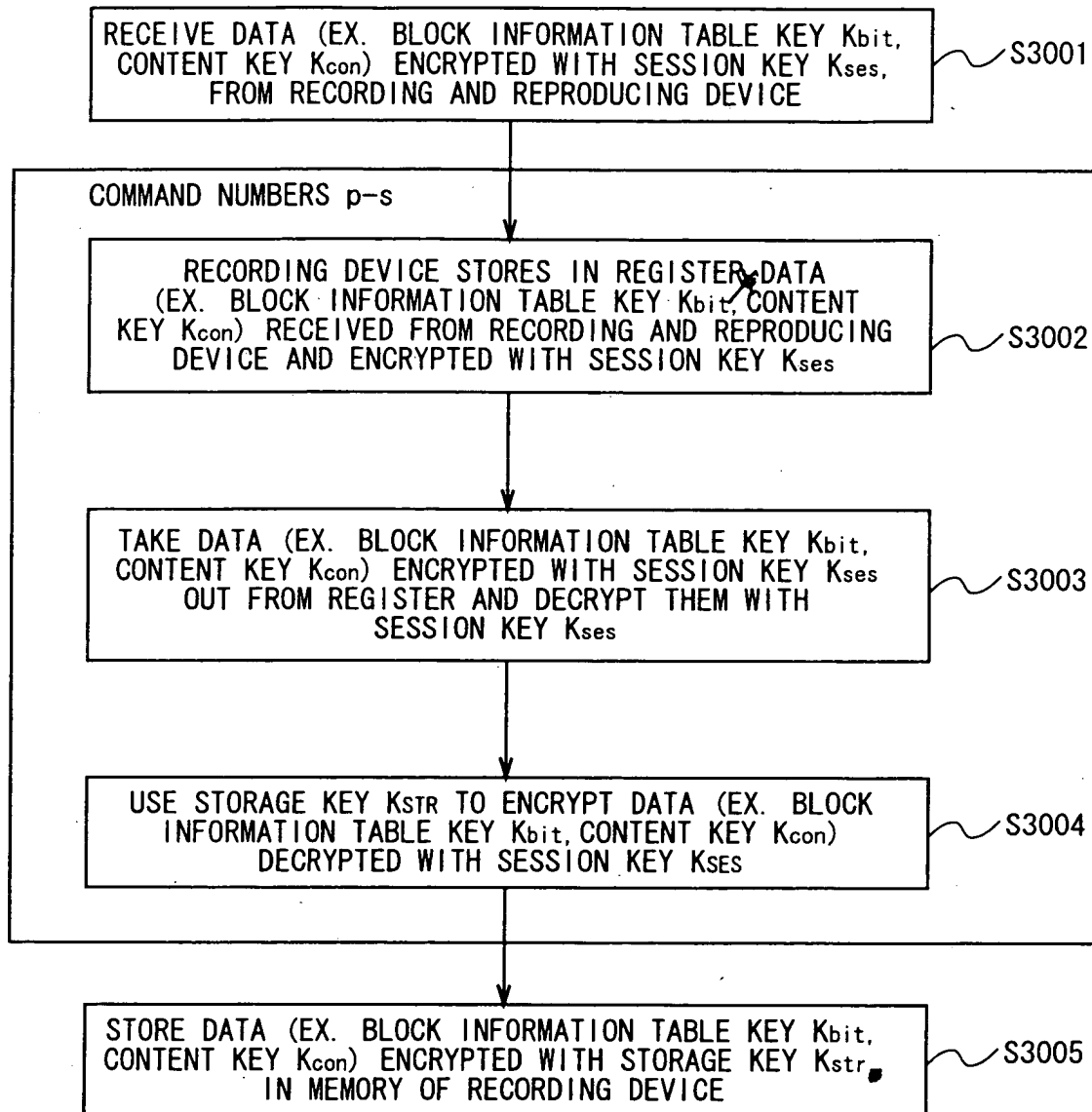


FIG. 30



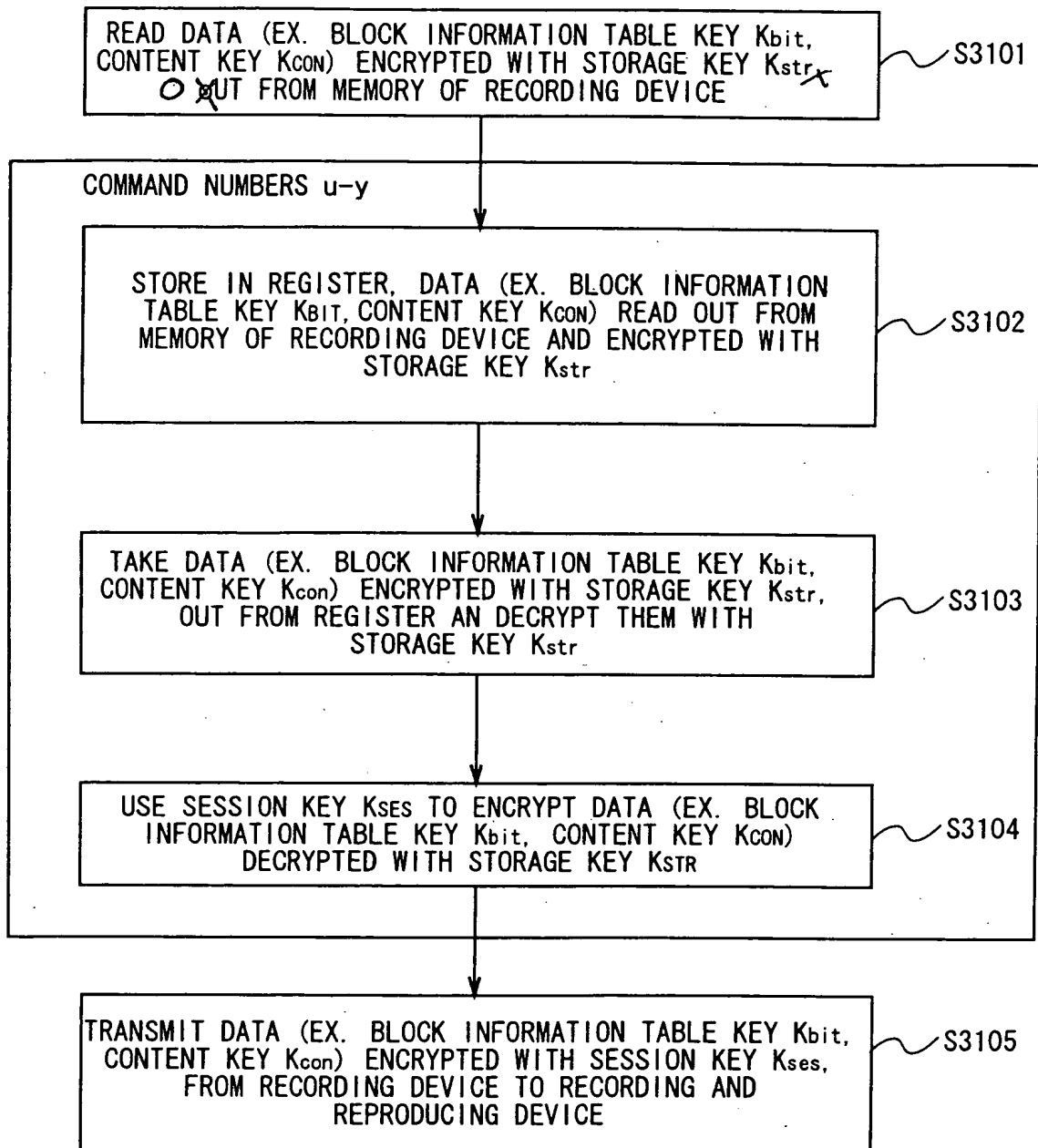
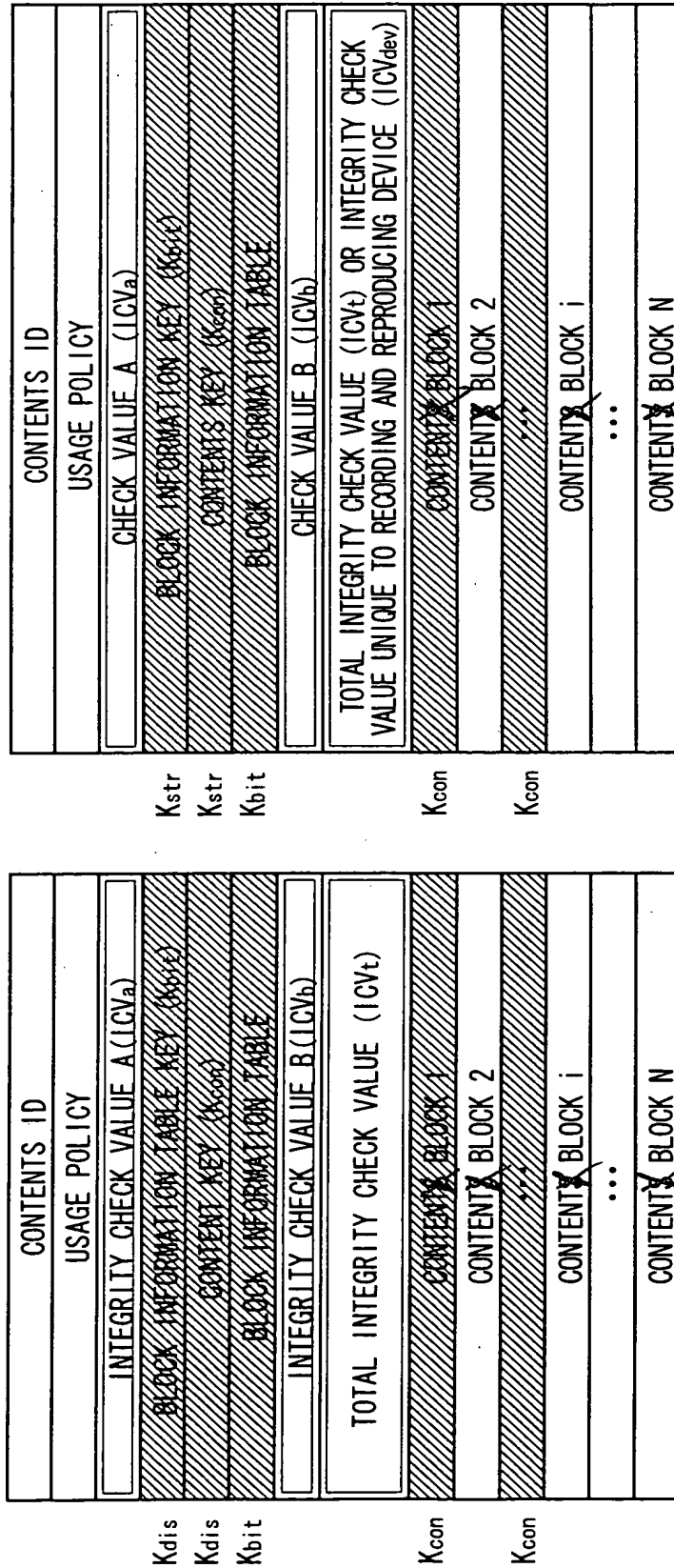


FIG. 31



FORMAT TYPE 0



DATA FORMAT ON MEDIUM AND COMMUNICATION PATH      CONTENT STORED IN RECORDING DEVICE



FIG. 32



FORMAT TYPE 1

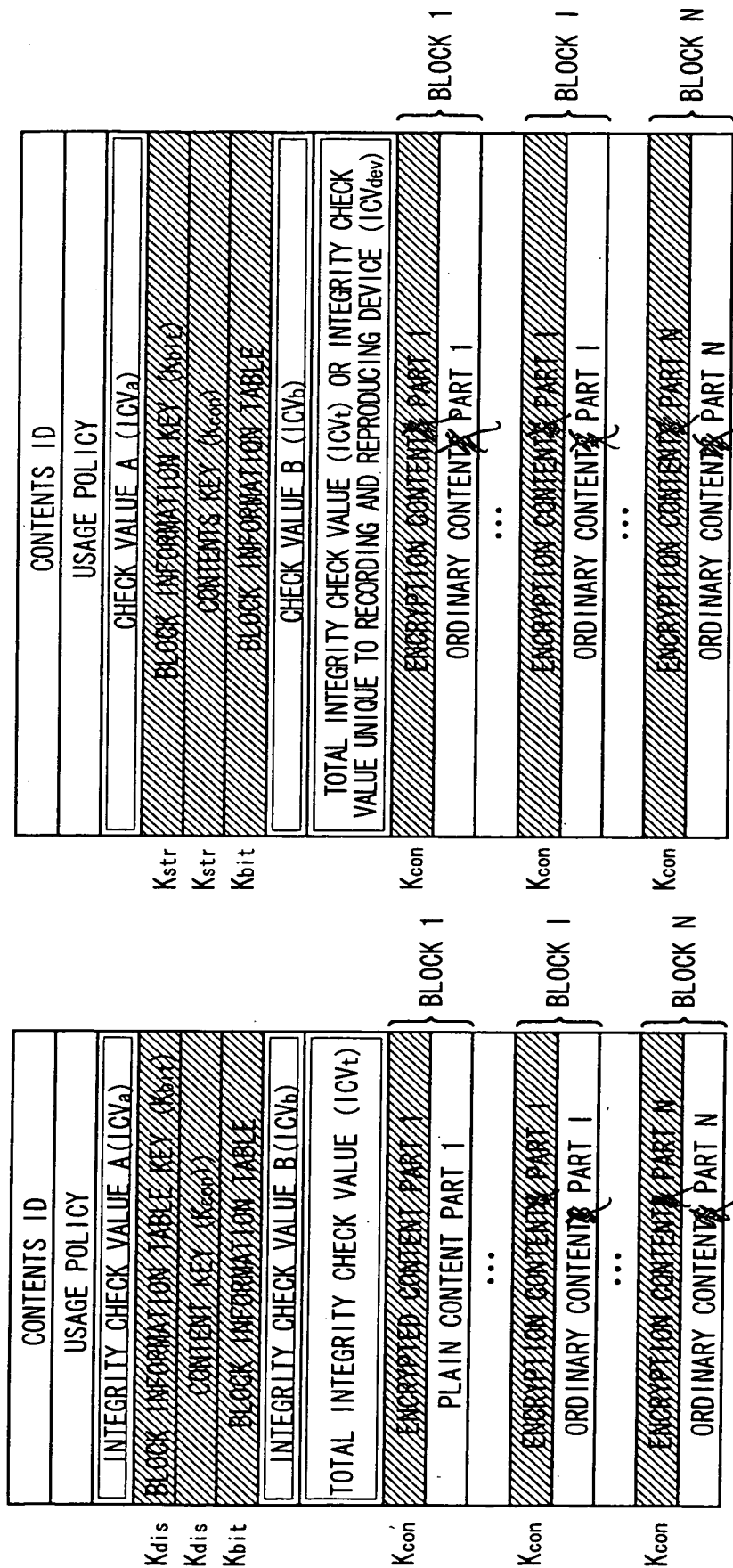


FIG. 33



FORMAT TYPE 2

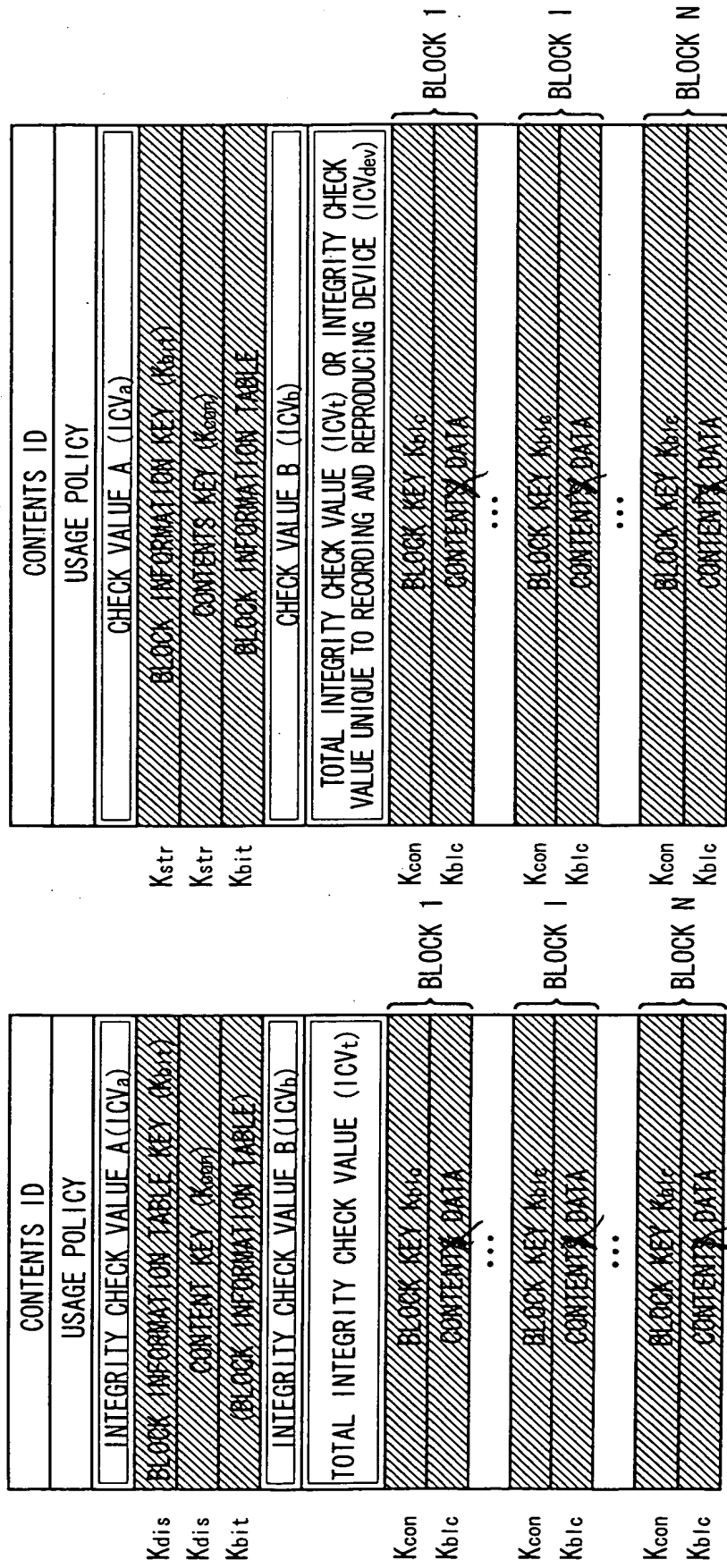
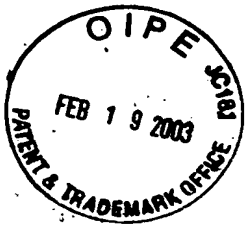


FIG. 34



FORMAT TYPE 3

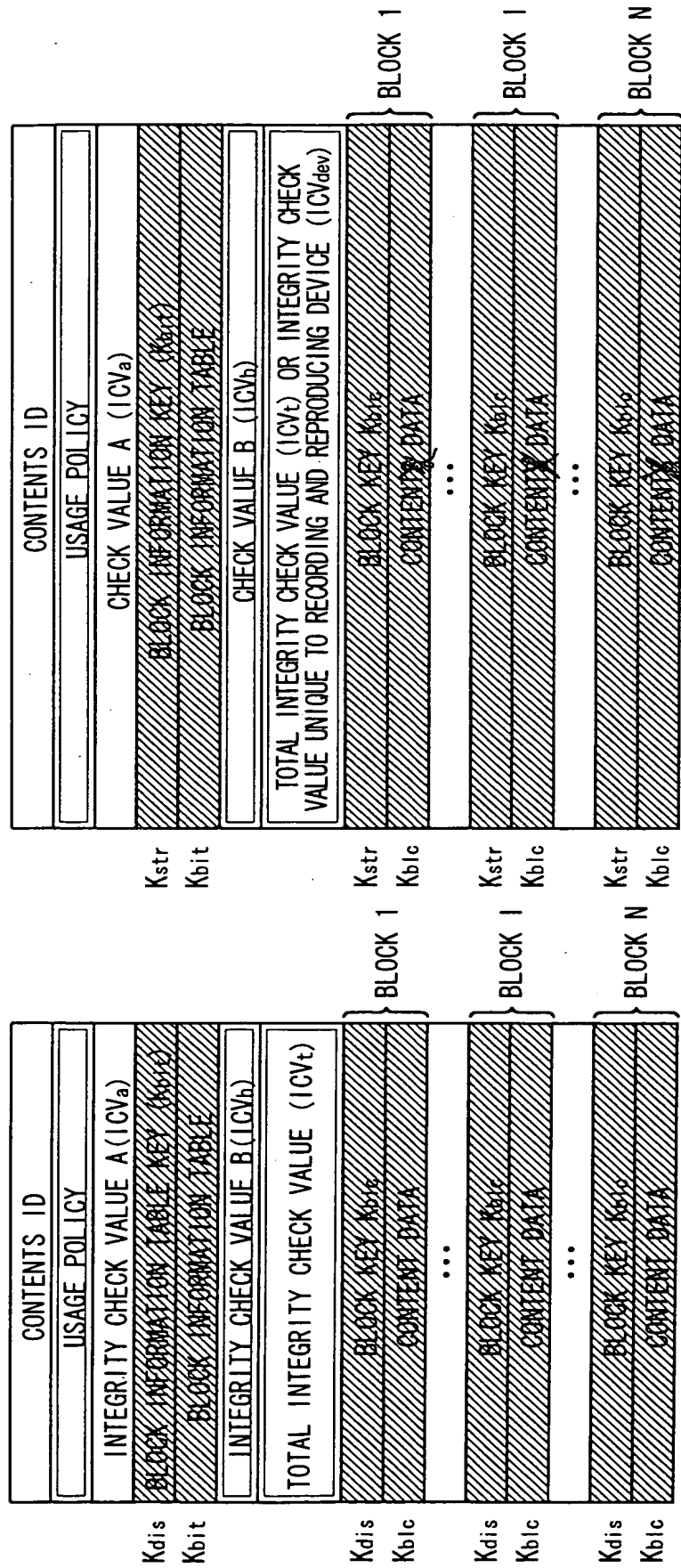


FIG. 35

# FORMAT TYPE 2 DOWNLOAD PROCESS

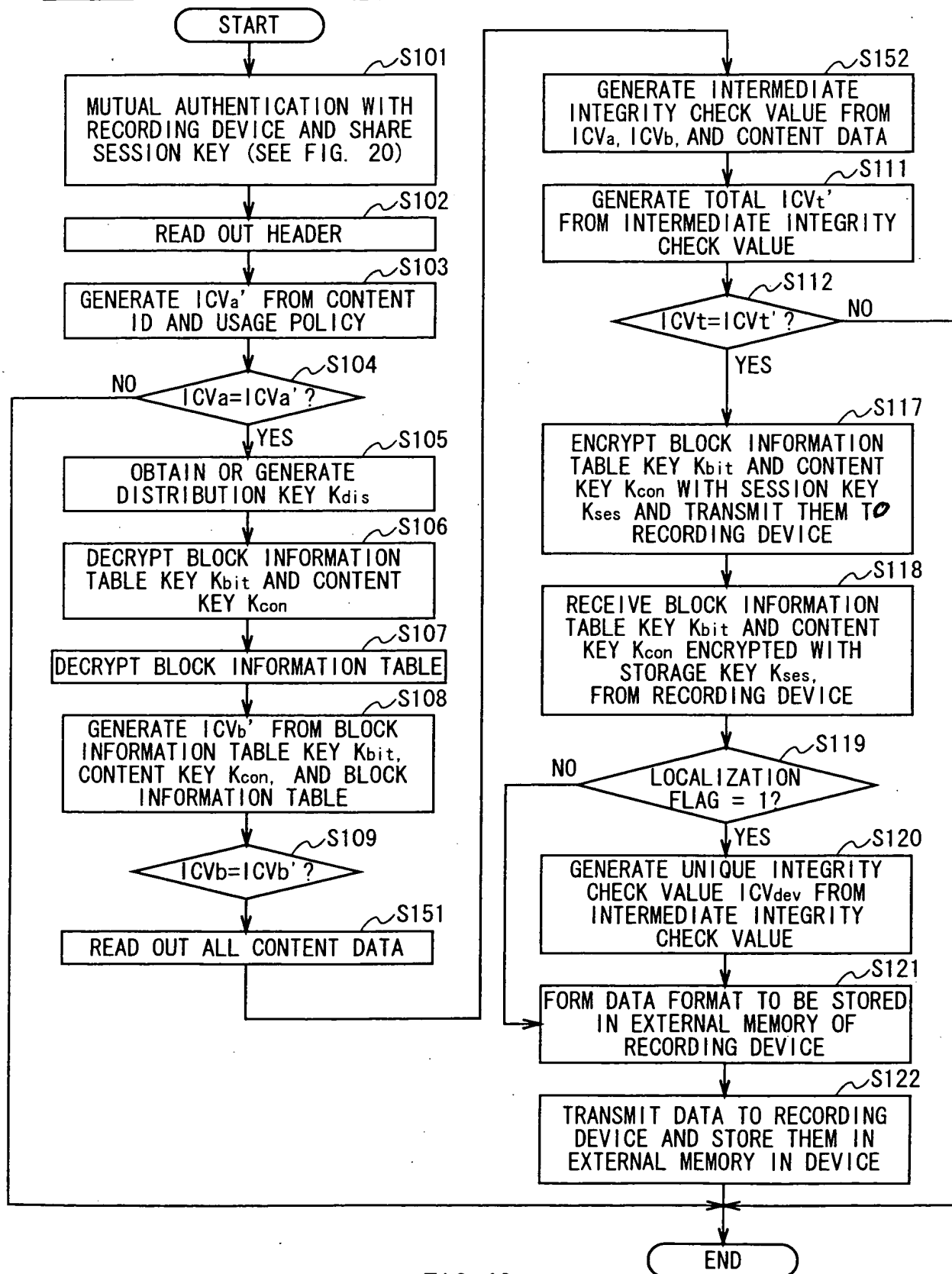


FIG. 40



FORMAT TYPE 1 REPRODUCTION PROCESS

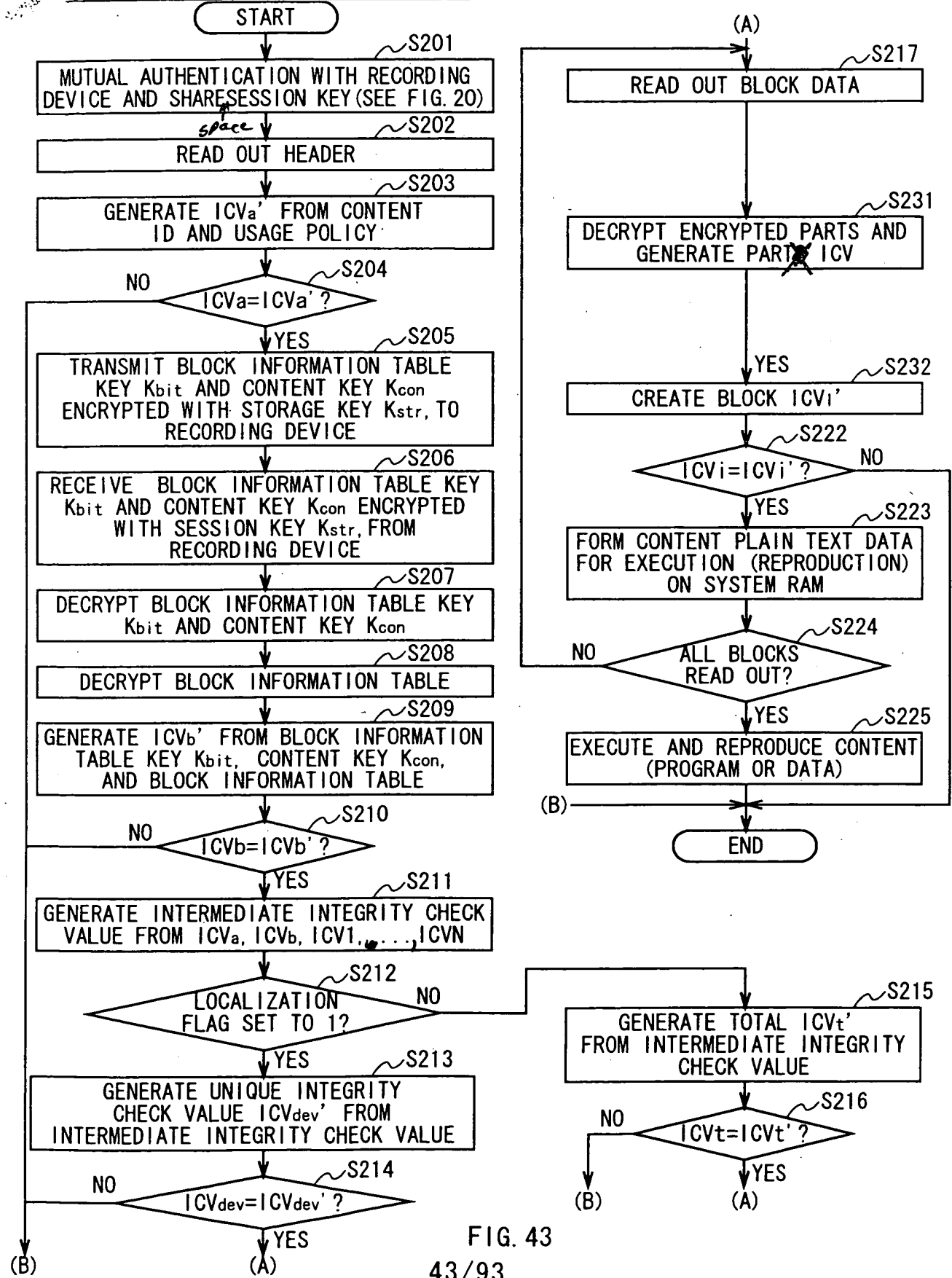


FIG. 43  
43/93



# FORMAT TYPE 2 REPRODUCTION PROCESS

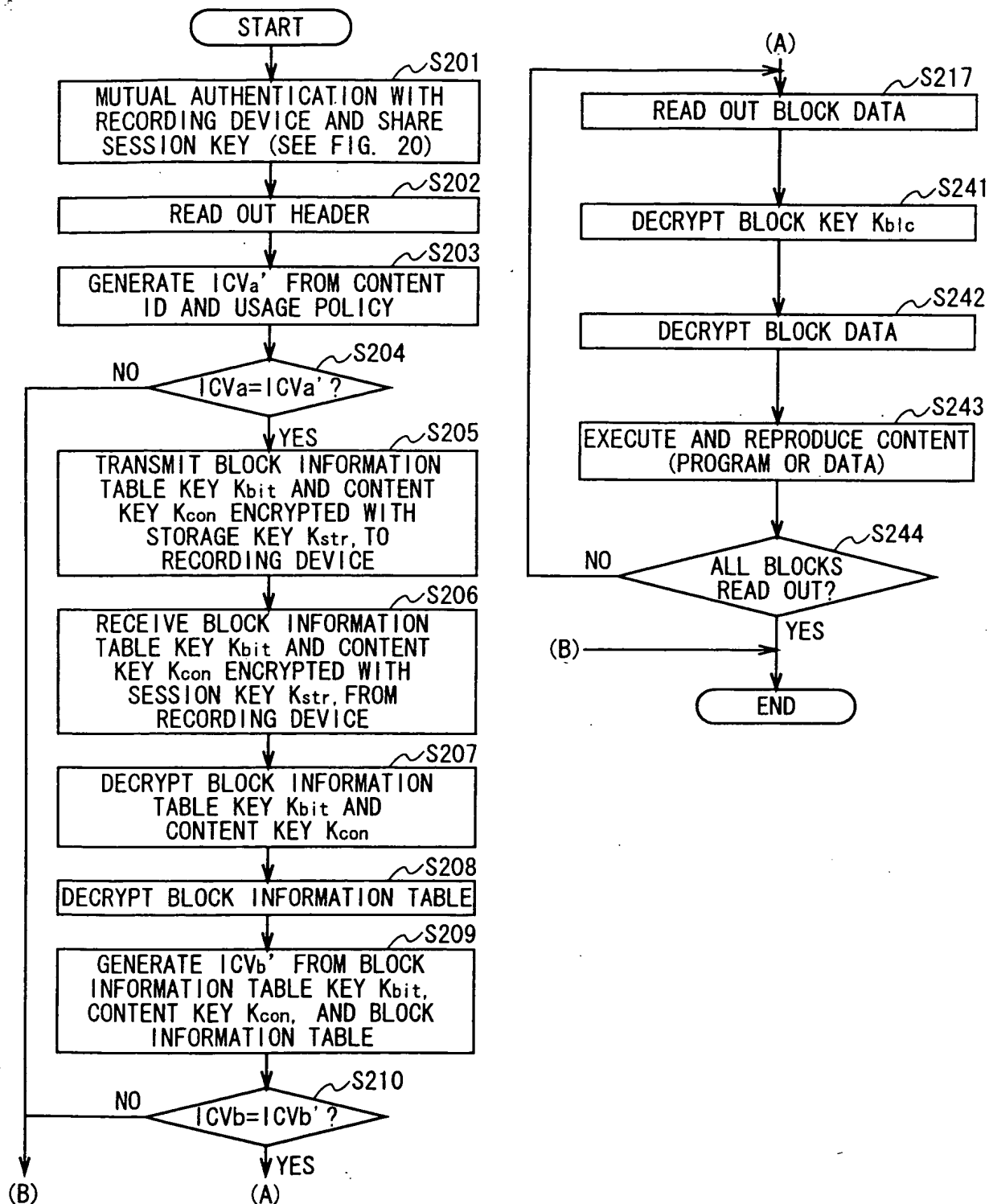


FIG. 44



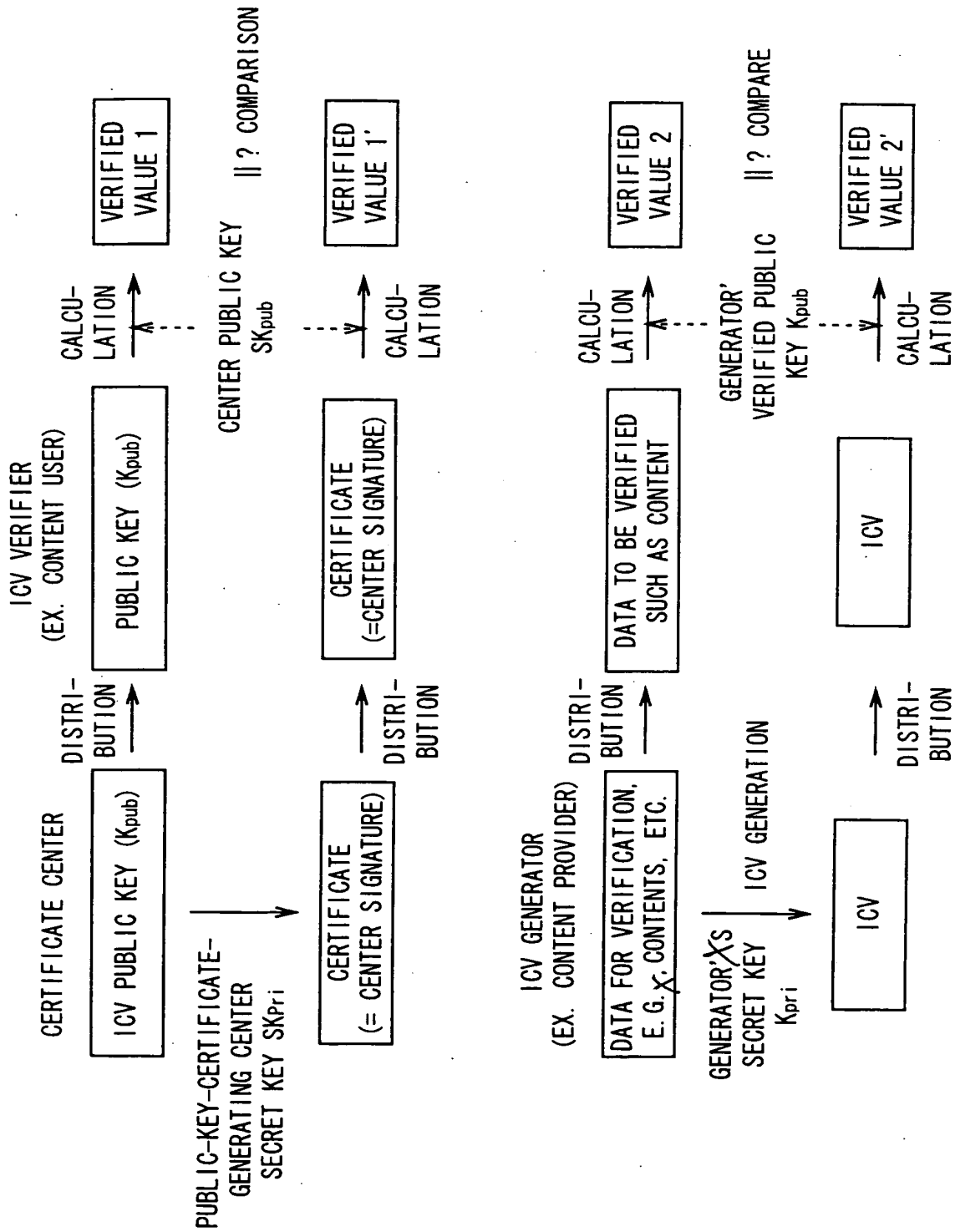


FIG. 48



# METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY - (2) [BASIC FLOW]

CONTENT PRODUCER OR MANAGER

START PRODUCING CONTENT

DETERMINE ID FOR CONTENT  
(CONTENT ID)

SELECT MASTER KEY MASTER KEY (EX.  
DISTRIBUTION-KEY-GENERATING  
MASTER KEY: MK<sub>dis</sub> 1, ... N)  
DEPENDING ON APPARATUS FOR WHICH  
USE OF CONTENT IS PERMITTED

GENERATE KEY (EX. DISTRIBUTION-  
KEY-GENERATING MASTER KEY: MK<sub>dis</sub>  
1, ... N) FROM MASTER KEY (EX.  
DISTRIBUTION-KEY-GENERATING  
MASTER KEY: MK<sub>dis</sub> 1, ... N)  
DEPENDENT ON APPARATUS FOR WHICH  
USE OF CONTENT IS PERMITTED  
AS WELL AS CONTENT ID

GENERATE ENCRYPTED CONTENTS  
C1, ... N FROM PART OR ALL OF  
CONTENT WITH KEY (EX. DISTRIB-  
UTION KEY K<sub>dis</sub> 1, ... N)

GROUP CONTENT ID, IDENTIFICATION  
INFORMATION FOR MASTER KEY  
USED, AND ENCRYPTED CONTENT INTO  
ONE DISTRIBUTED UNIT

END PRODUCING CONTENT

USER DEVICE

START USING CONTENT

DISTRIBUTED MASTER KEY  
IDENTIFICATION INFORMATION  
MATCH WITH OWNED MASTER KEY?

END

READ OUT CONTENT ID

GENERATE KEY (EX. DISTRIBUTION  
K<sub>dis</sub>) FROM CONTENT ID AND  
MASTER KEY (EX. DISTRIBUTION-  
KEY-GENERATING MASTER KEY: MK<sub>dis</sub>)

DECRYPT ENCRYPTED PART OF  
CONTENT WITH KEY (EX. DISTRIBU-  
TION KEY K<sub>dis</sub>)

USE CONTENT

END USING CONTENT

## [KEY OWNER CONFIGURATION]

CONTENT PRODUCER OR MANAGER

MASTER KEY  
(EX. DISTRIBUTION-KEY-  
GENERATING MASTER KEY: MK<sub>dis</sub>)

SHARE

USER DEVICE

MASTER KEY  
(EX. DISTRIBUTION-KEY-  
GENERATING MASTER KEY: MK<sub>dis</sub>)

CONTENT ID

ID PROTECTED  
CONTENT

FIG. 51

50/93

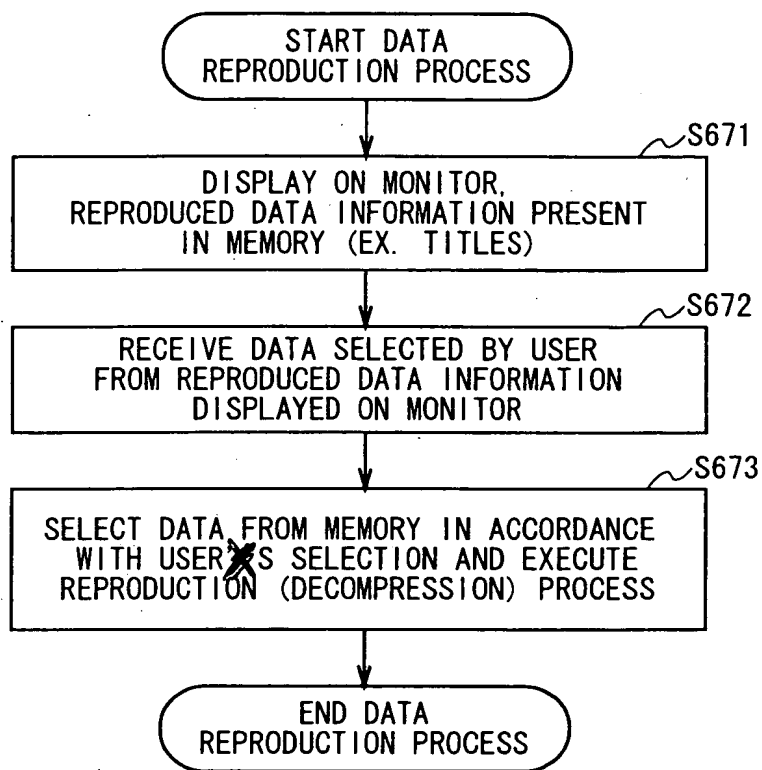


FIG. 62

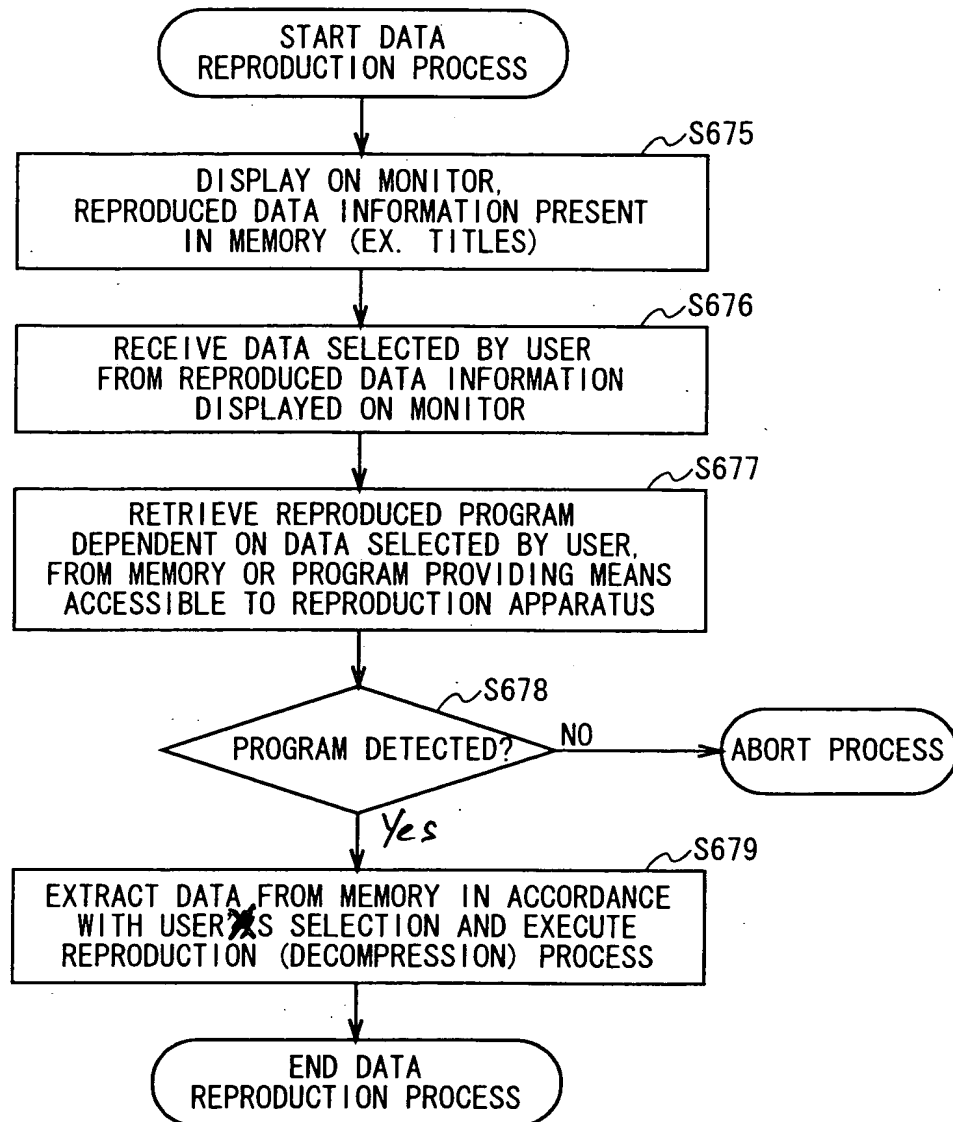
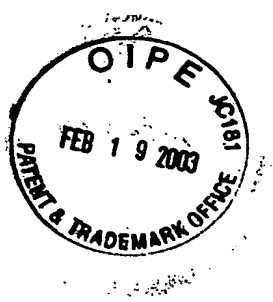


FIG. 64

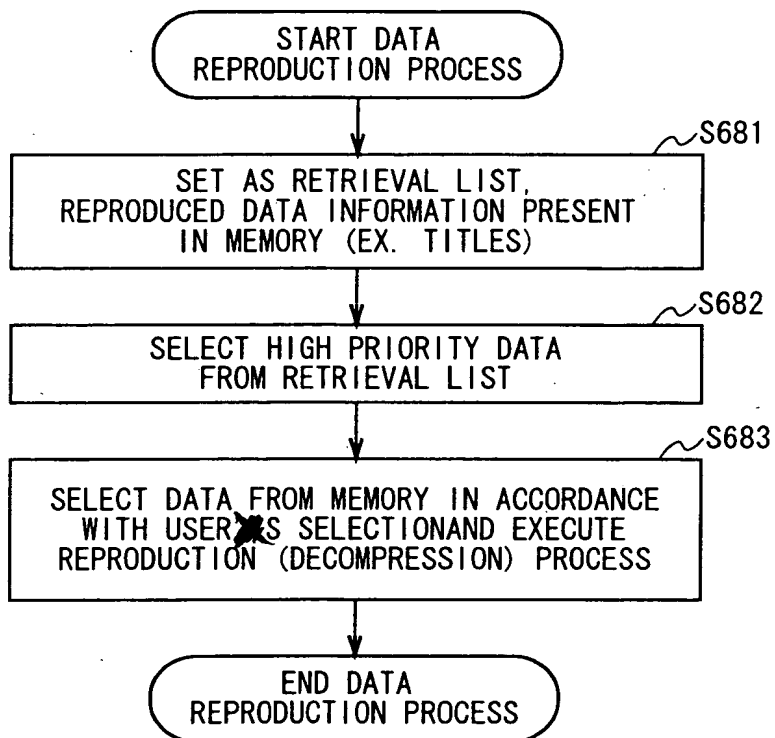
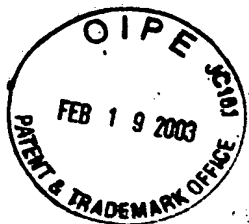


FIG. 66

EXAMPLE OF CONTENT CONFIGURATION (4)

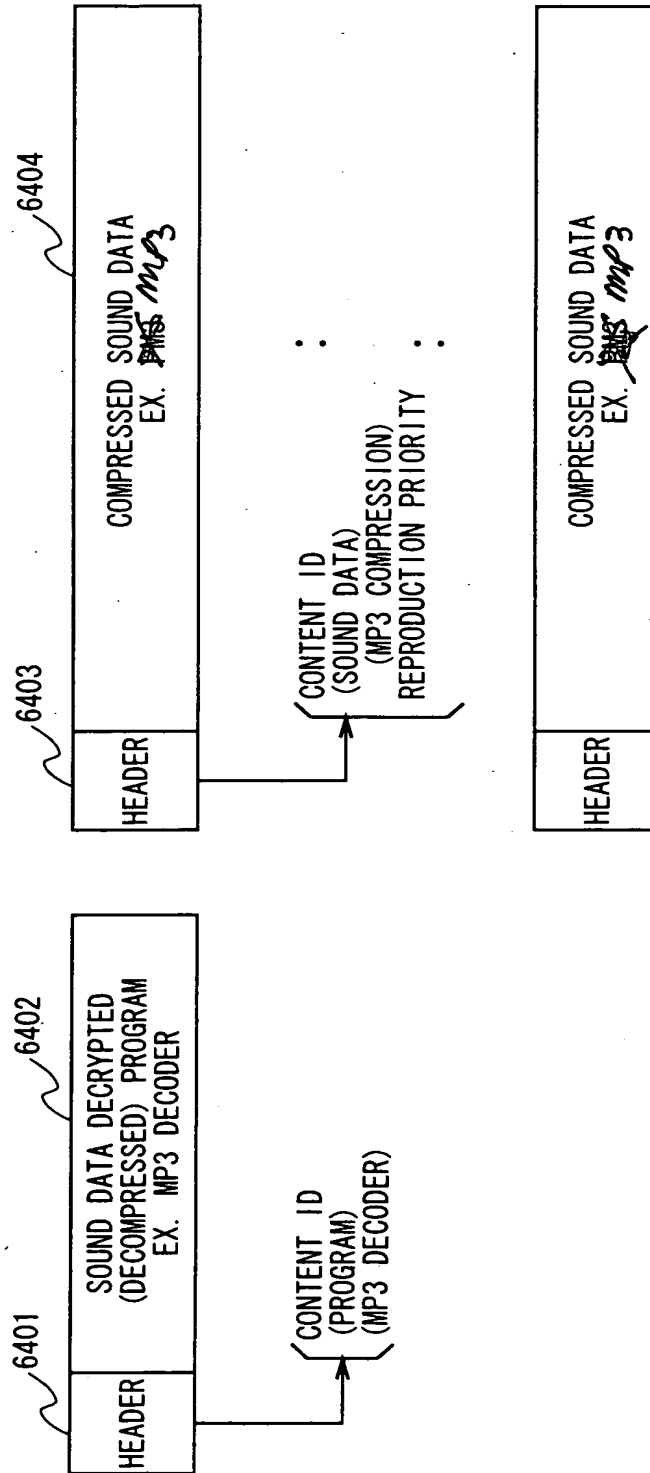


FIG. 67

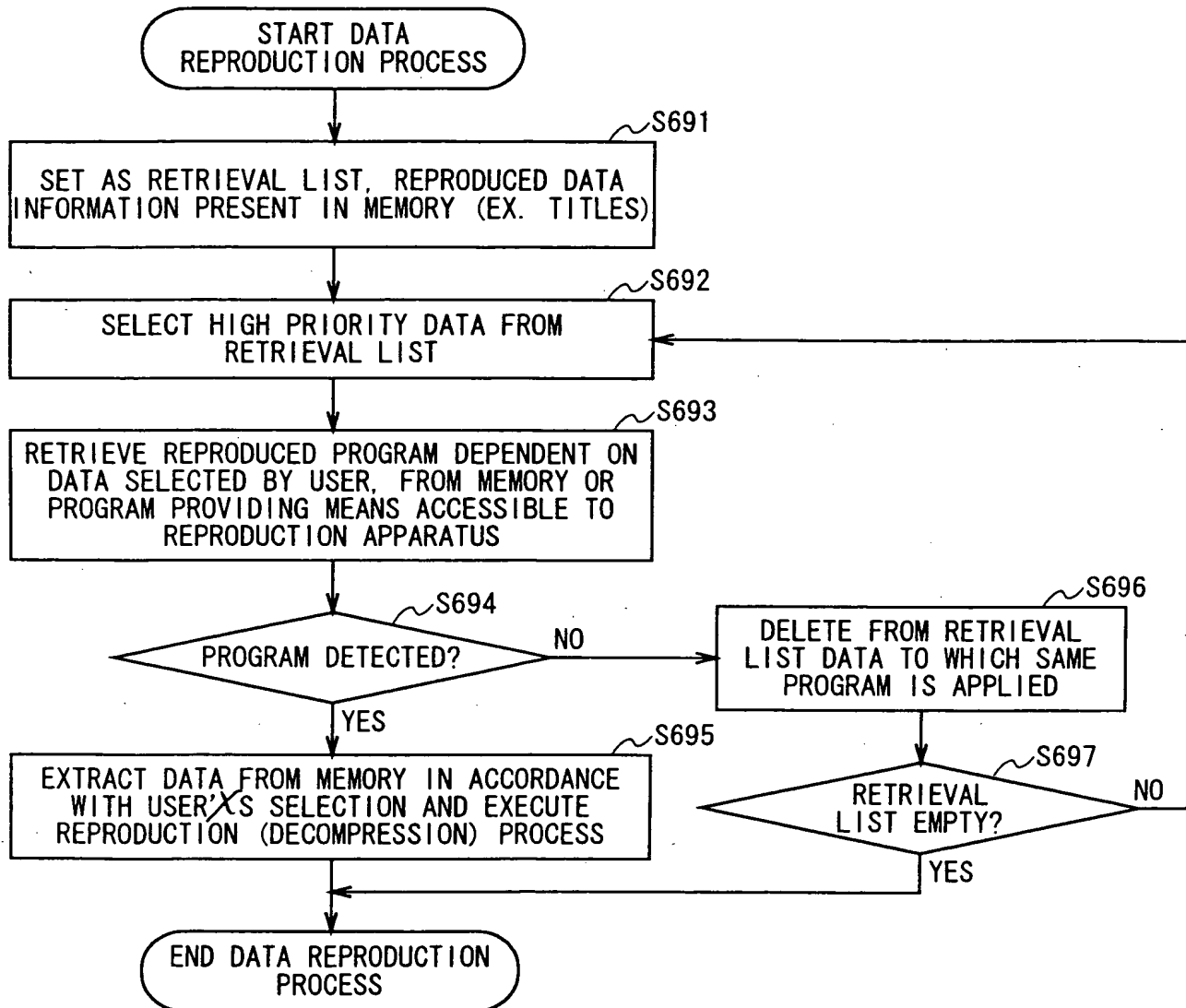


FIG. 68



(2) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT UNIQUE KEY OR SYSTEM COMMON KEY

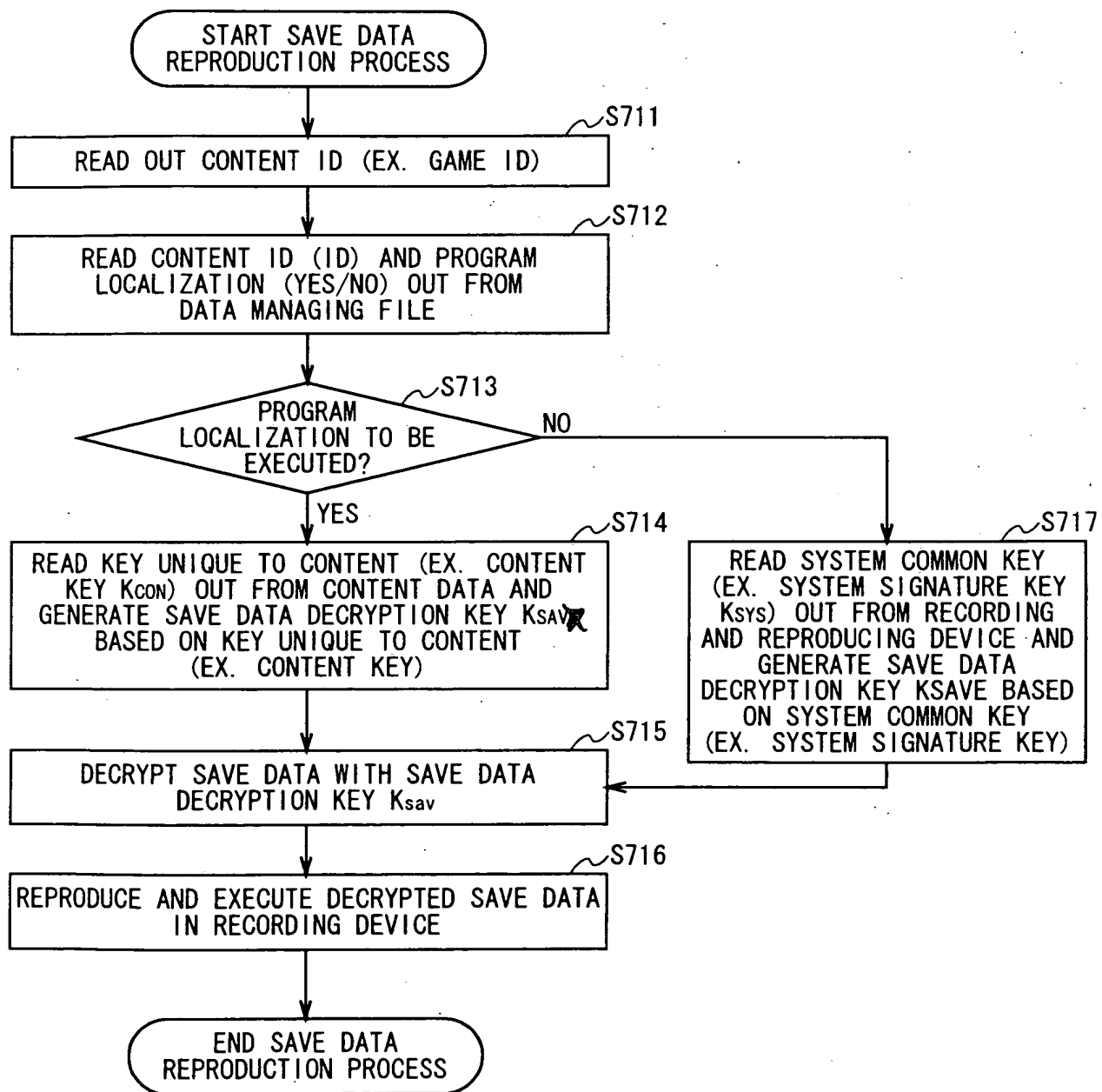


FIG. 72





(3) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENT ID OR SYSTEM COMMON KEY

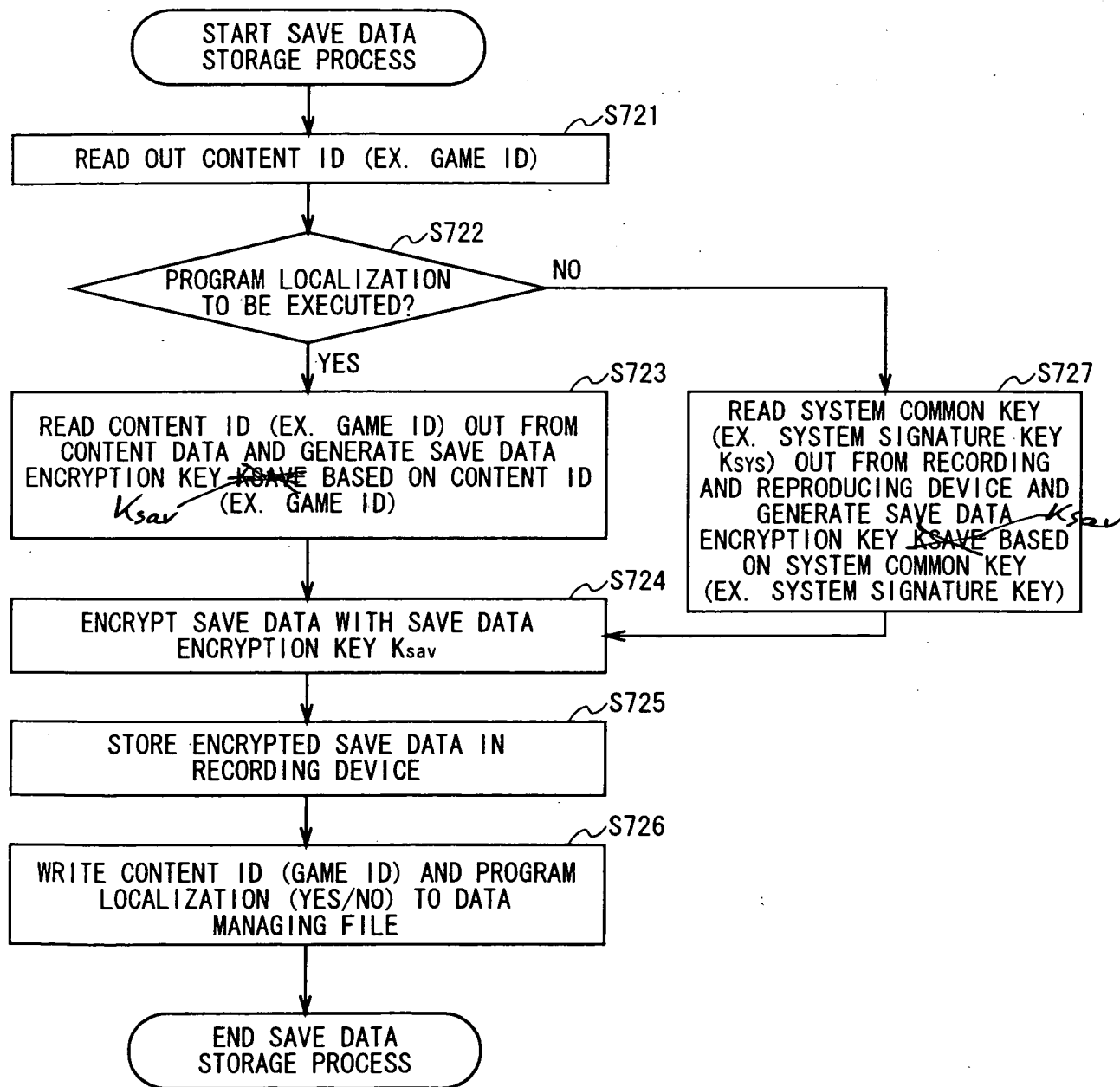


FIG. 73



(4) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT ID OR SYSTEM COMMON KEY

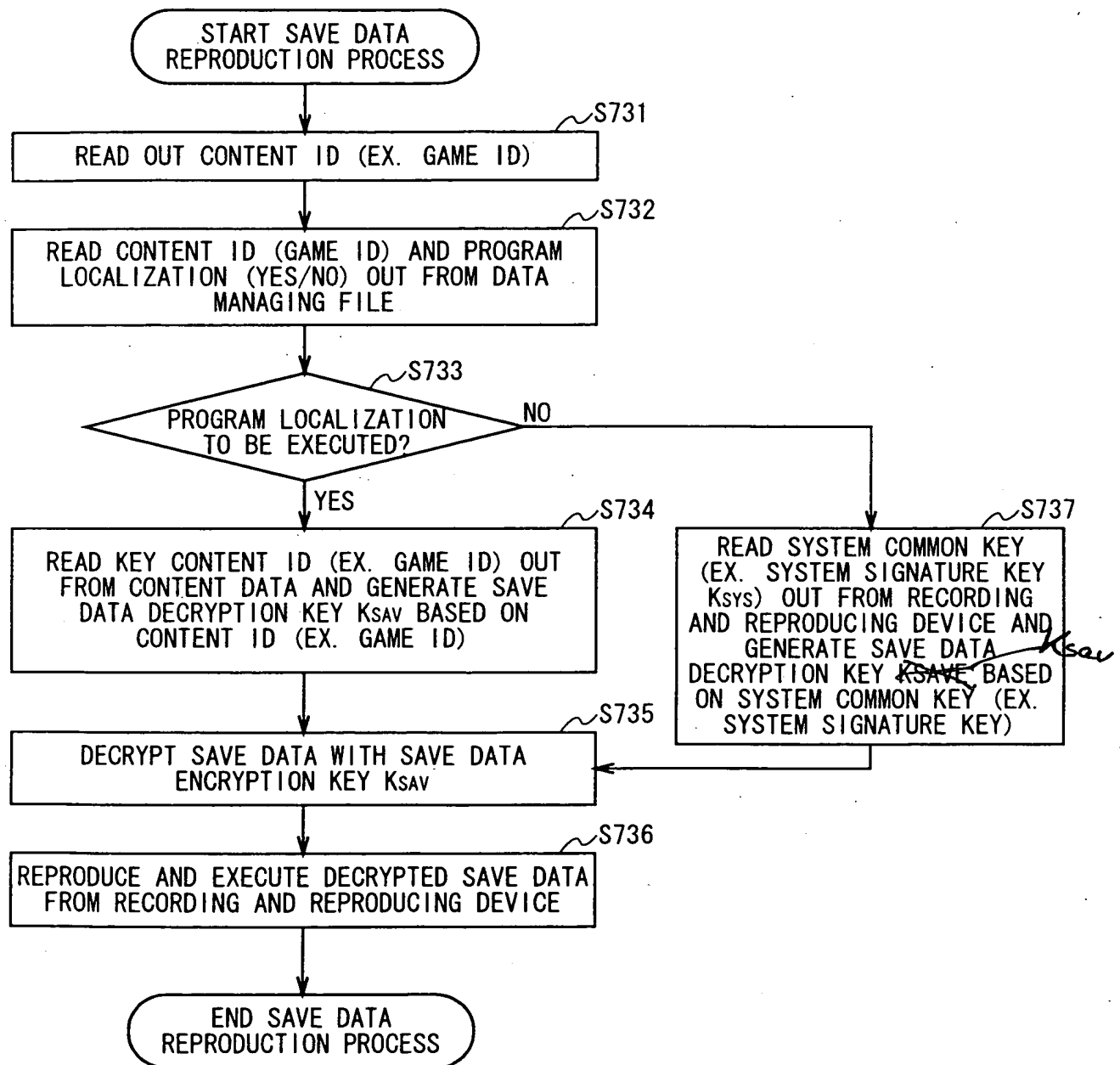


FIG. 74

(5) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORDING AND REPRODUCING DEVICE UNIQUE KEY OR SYSTEM COMMON KEY

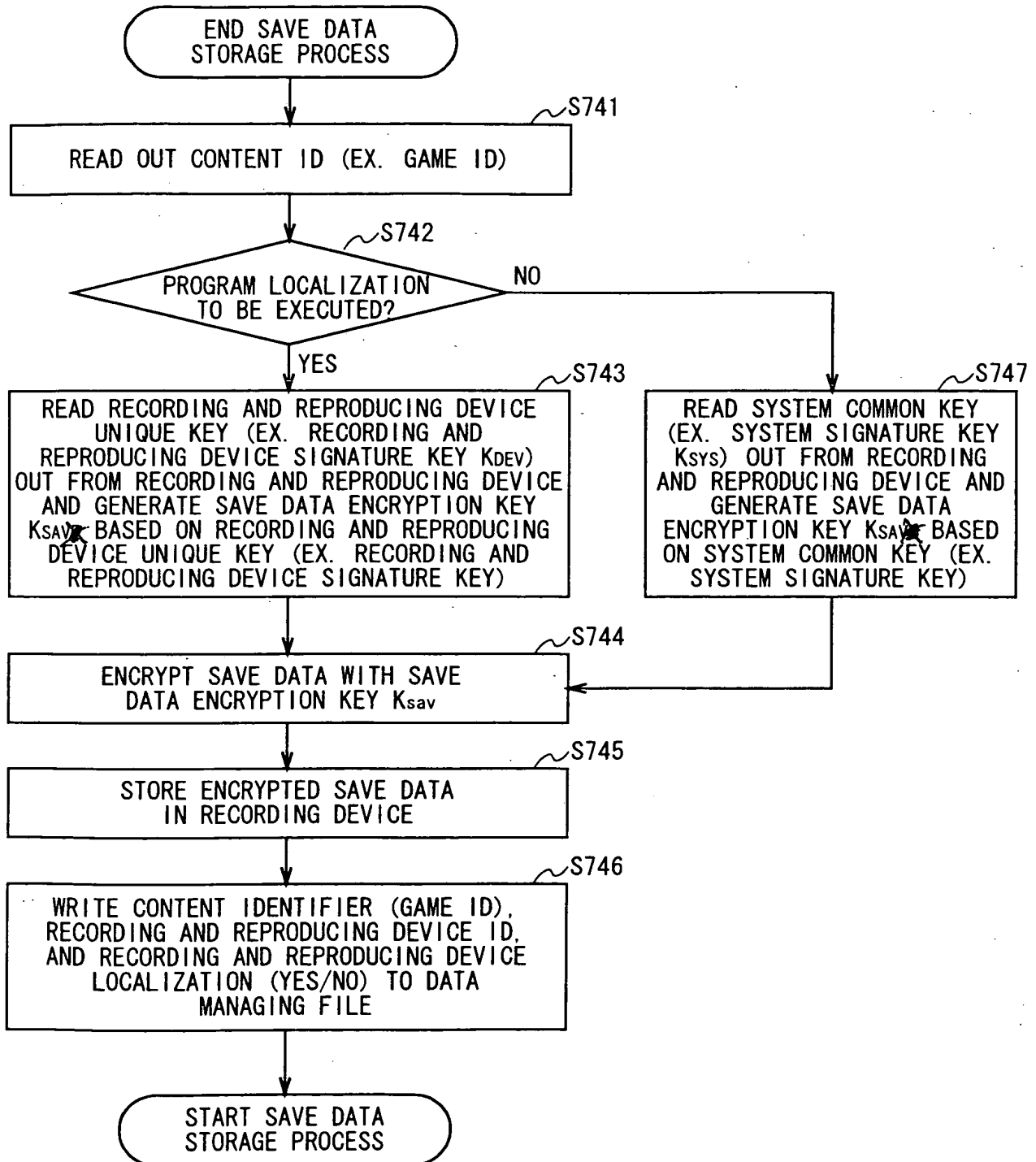


FIG. 75

(6) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORDING AND REPRODUCING DEVICE UNIQUE KEY OR SYSTEM COMMON KEY

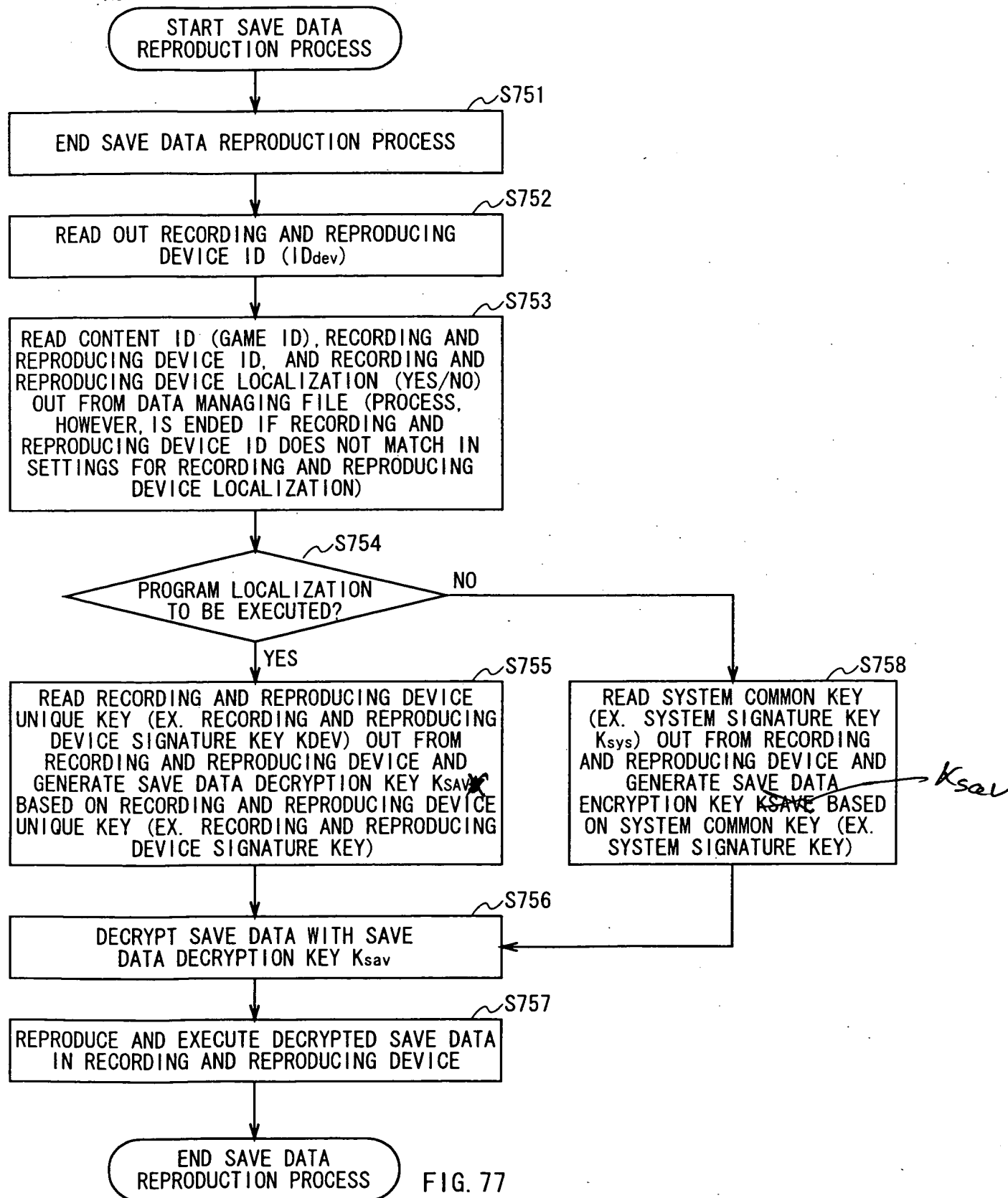


FIG. 77

(7) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORDING AND REPRODUCING DEVICE ID OR SYSTEM COMMON KEY

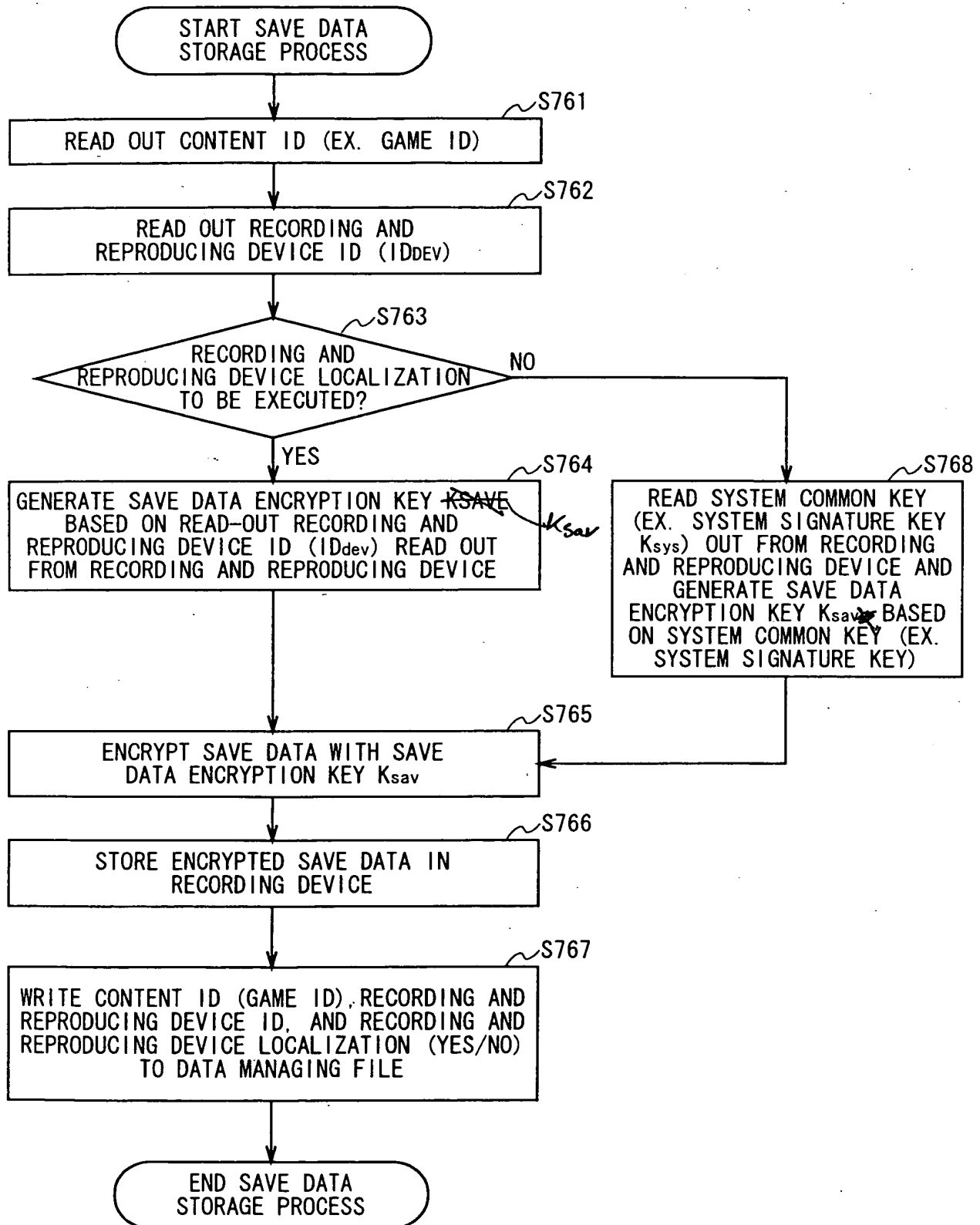


FIG. 78



(8) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORDING AND REPRODUCING DEVICE ID OR SYSTEM COMMON KEY

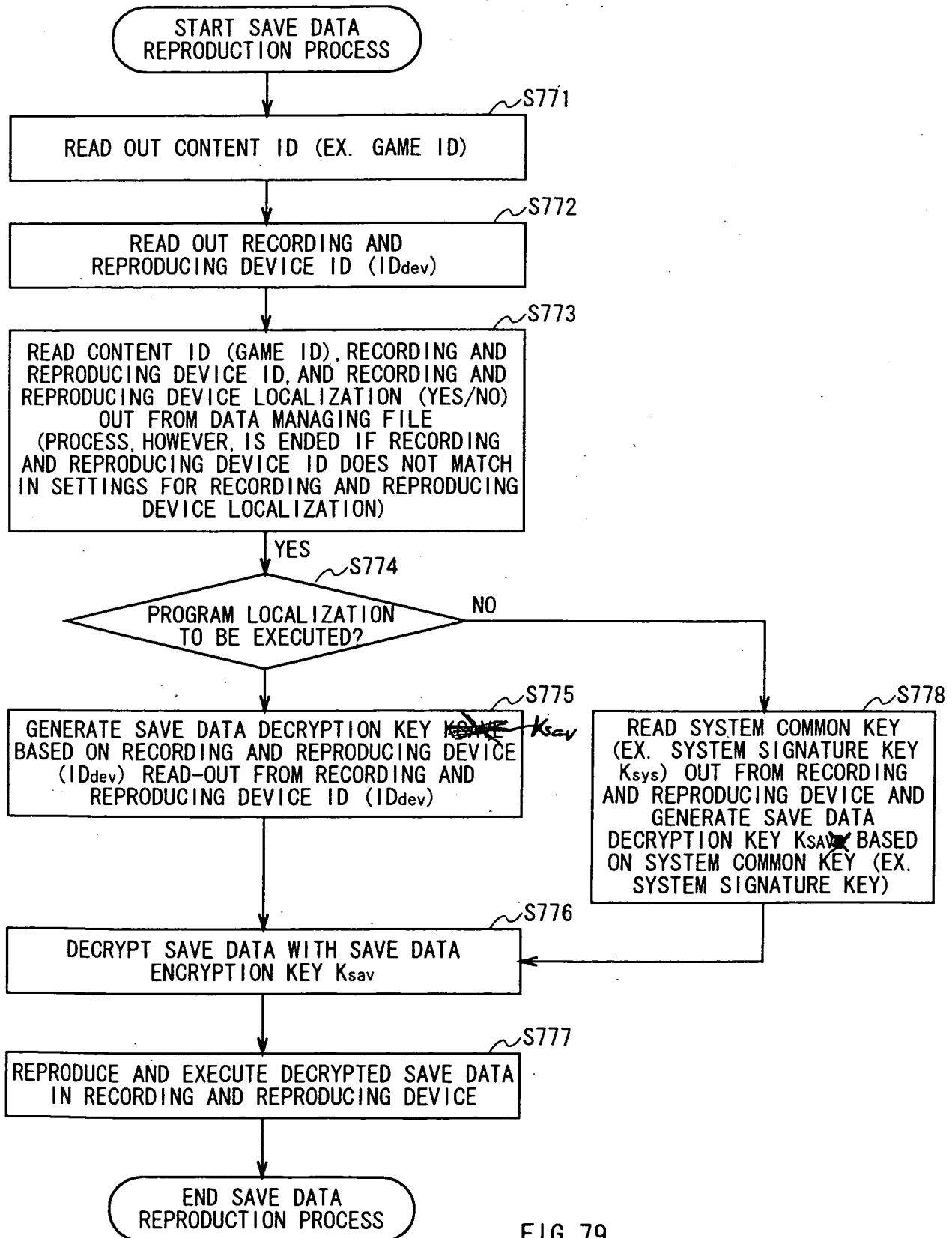


FIG. 79

(9) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENT UNIQUE KEY, RECORDING AND REPRODUCING DEVICE UNIQUE KEY, OR SYSTEM COMMON KEY

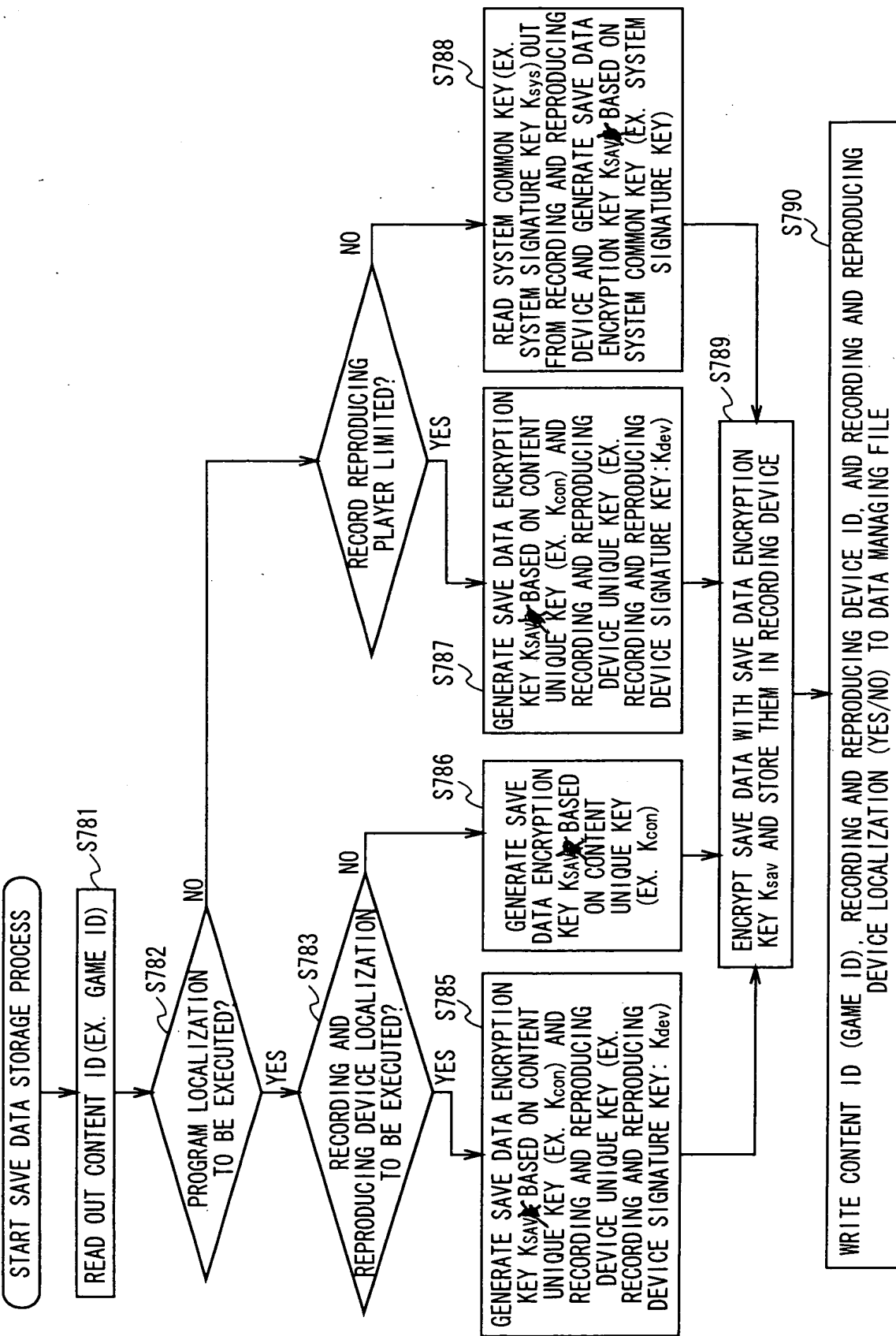


FIG. 80

(10) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT UNIQUE KEY, RECORDING AND REPRODUCING DEVICE UNIQUE KEY, OR SYSTEM COMMON KEY

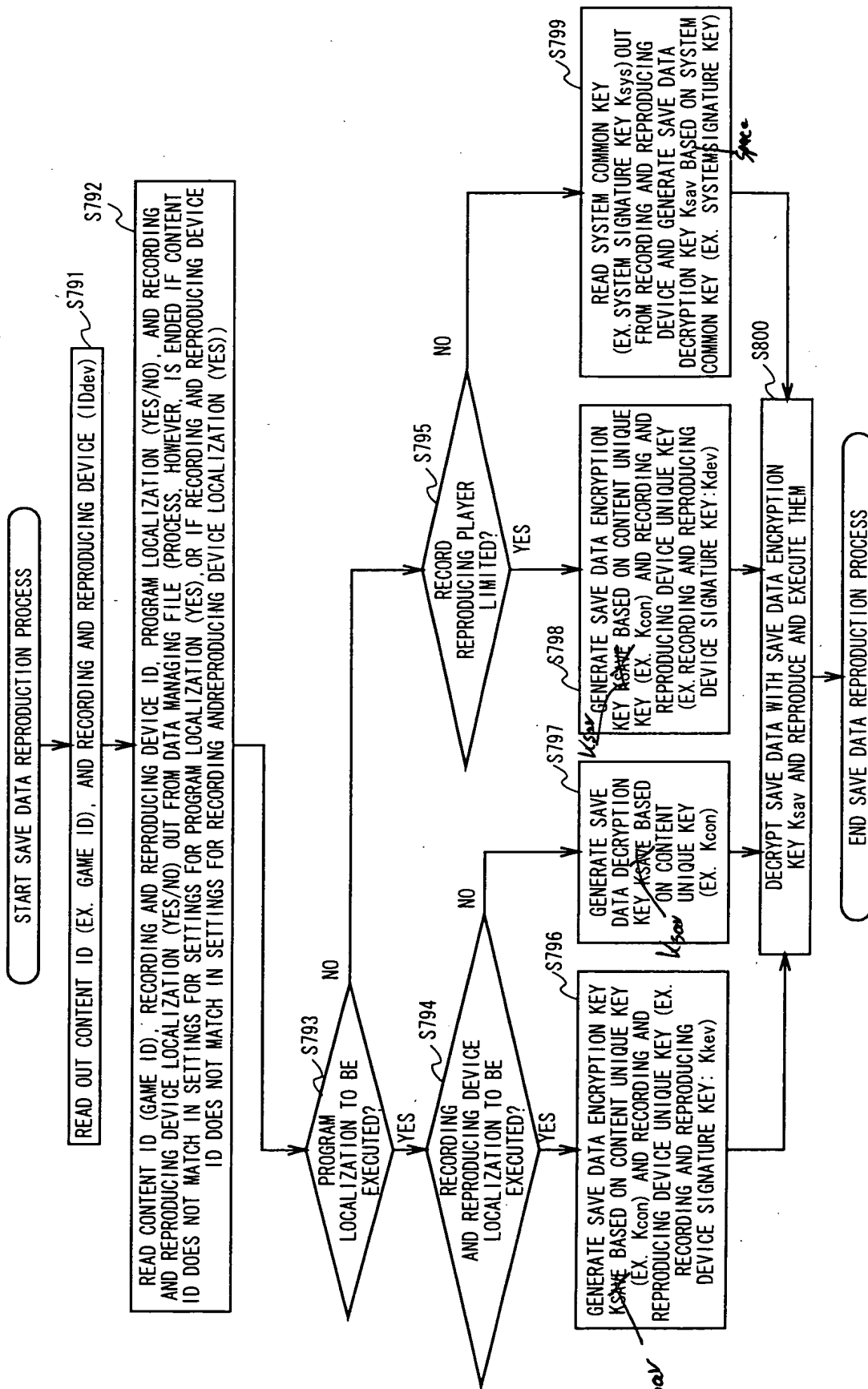


FIG. 82





(12) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING USER PASSWORD OR SYSTEM COMMON KEY

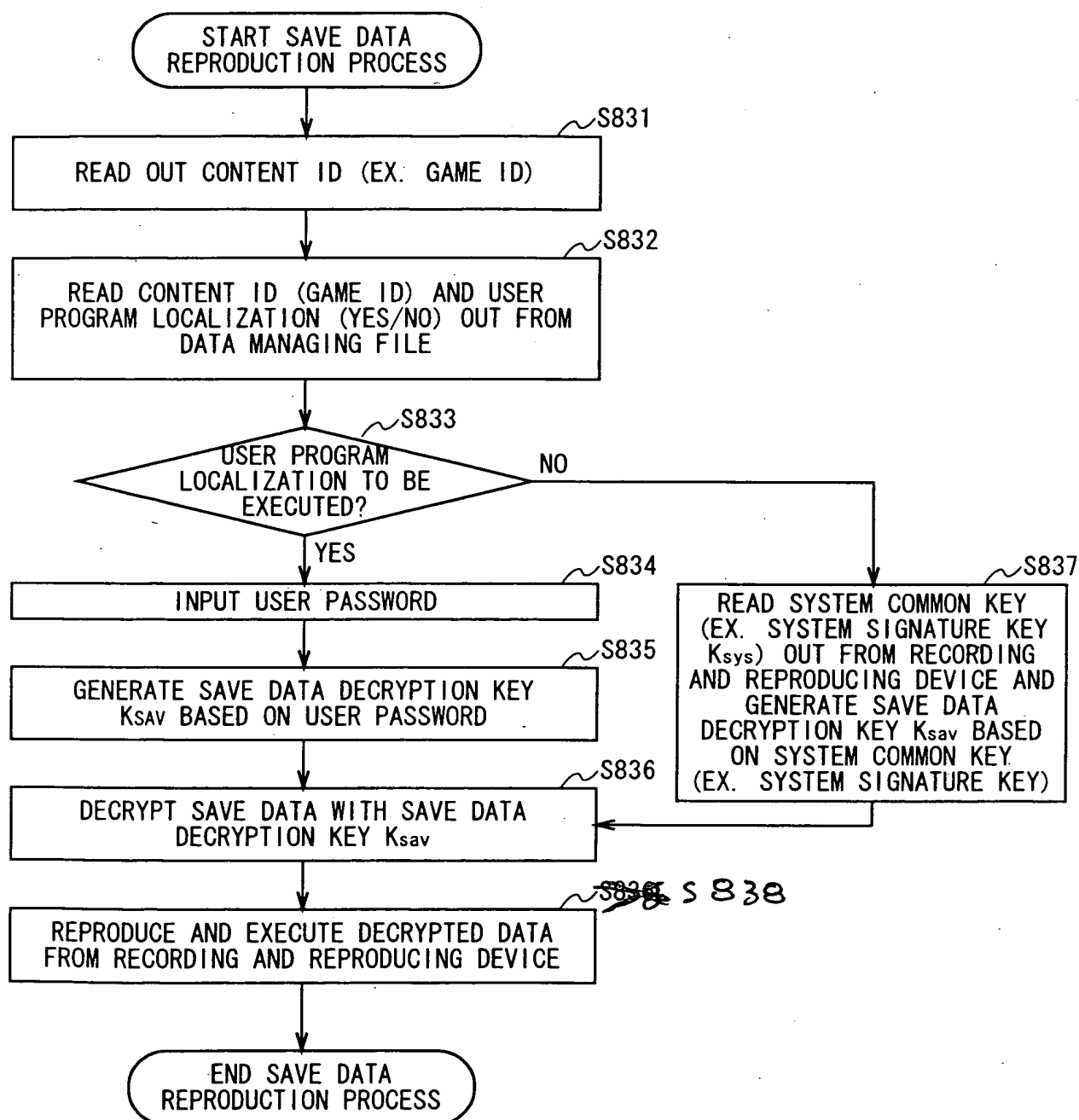


FIG. 85

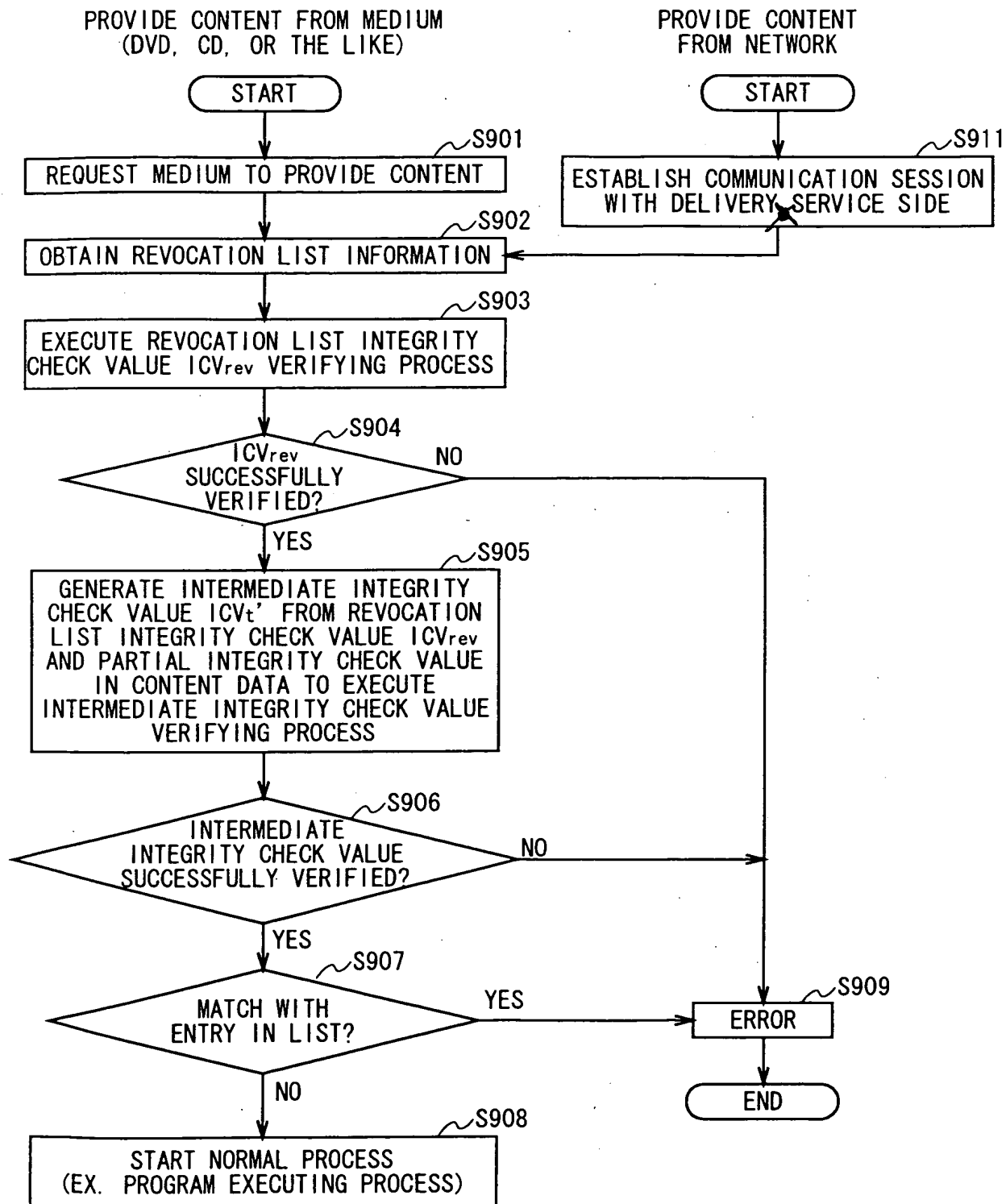


FIG. 87



PROVIDE CONTENT FROM RECORDING  
DEVICE (MEMORY CARD OR THE LIKE)

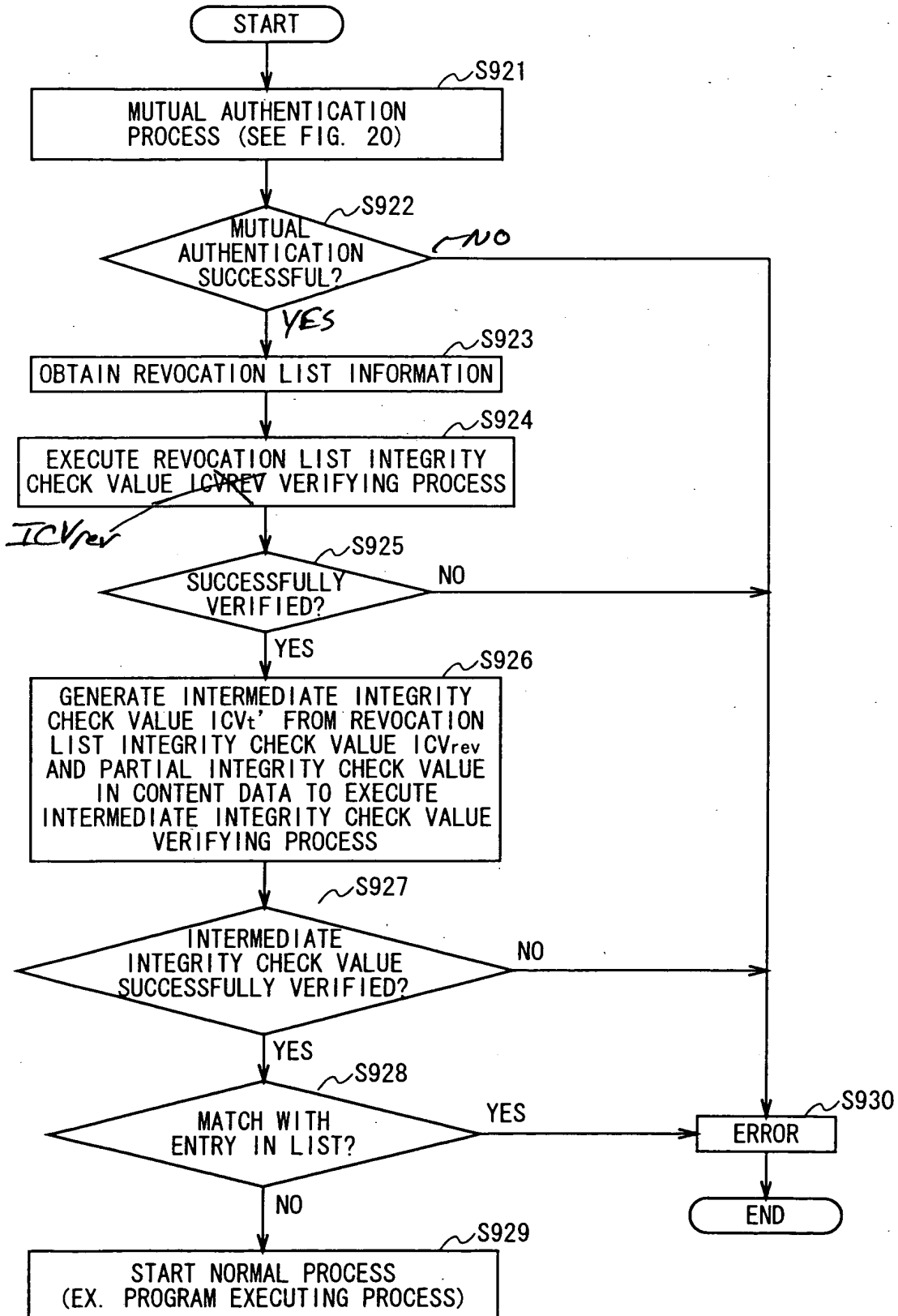


FIG. 88  
87/93